环球律师事务所
GLOBAL LAW OFFICE

CAICT 中国信通院

个性化展示安全与合规报告

2020年9月

版权声明

撰写团队

编写单位（按首字母顺序）：

北京市环球律师事务所、南都个人信息保护研究中心、中国信息通信研究院安全研究所。

编写组成员（按首字母顺序）：

陈湉、蒋琳、李慧琪、孟洁、娜迪娅、王程、殷坤、尤一炜、张淑怡

联系人及联系方式：

陈湉

电话：010-6230 8820

邮箱：chentian@caict.ac.cn

蒋琳

电话：010-5954 0274

邮箱：jianglin@nandu.cc

孟洁

电话：010-6584 6768

邮箱：mengjie@glo.com.cn

前言

个性化展示是当今互联网领域最重要的信息技术之一，它通过对用户的跟踪识别进行精准画像，实现向用户定向推送符合其喜好的产品和/或服务的目的。以电子商务领域中的亚马逊、淘宝等世界知名电子商务平台为例，个性化展示以及推送所带来的订单转化率已经逐渐超过传统的营销方式，足以彰显该技术在当下运用之广泛。

个性化展示为用户解决了信息过载的问题，同时也帮助企业创造了难以估量的财富。然而，在用户个人信息收集和使用的过程中，企业不正当使用或泄露个人信息等问题却始终困扰着该技术的健康发展。为此，我国颁布多部法律法规以及国家标准，规范个性化展示、程序化广告、新闻资讯或商业广告的个性化展示以及定向推送等相关问题，目的就在于打击这些个人信息不正当利用的乱象。

本报告聚焦于个性化展示技术，通过对实践中常用的20款App进行测评，观察我国企业在利用个性化展示技术时，对用户个人信息保护的现状。同时，本报告结合实际案例，分析个性化展示涉及的主要合规问题，以及企业在使用该技术过程中面临的法律合规风险。通过调研欧盟、美国的相关经验做法，从法律法规、企业责任、行业自律等方面，结合我国实际情况提出了有针对性的建议。

目录

一、个性化展示的业内现状 8

（一）电商类 8

（二）短视频类 9

（三）新闻资讯类 9

（四）金融服务类 10

（五）外卖类 11

二、个性化展示的法律规制 12

（一）法律法规 12

（二）监管动态 15

三、常见应用的个性化展示合规情况测评 17

（一）测评方法 17

（二）测评结果 19

四、个性化展示主要问题及分析 28

（一）法律层面：术语零散不统一 28

（二）技术层面：难以删除或进行匿名化处理 29

（三）企业合规层面：未能履行个人信息处理的相关要求 31

五、个性化展示合规管理的域外经验 38
（一）欧盟部分 38
（二）美国部分 43
六、针对我国关于个性化展示的合规建议 51
（一）尽快完善法律法规或国家标准，统一个性化展示行为的概念 51
（二）个人信息收集应当符合透明性原则，保障用户的知情同意权 51
（三）保障用户的自主控制权 52
（四）保障用户被处理个人信息的安全 53
（五）个人信息的共享需征得用户同意 54
（六）鼓励企业开展行业自律 55
（七）建立有效的问责机制 55
附录：相关定义列表 58

一、个性化展示的业内现状

随着技术的普及与应用，“千人千面”的个性化展示愈加渗透到公众生活的方方面面，也在改变公众获取信息的方式。举着手机，滑滑屏幕，看新闻，淘宝贝，搜话题，买票订饭，用户在网上的所看、所做，都可能被App打上标签，最终形成一幅用户“画像”。大数据算法通过对个人网络痕迹的收集与分析，帮助用户在海量信息中筛选出可能是自己最想看到的内容，这大大降低了信息精准匹配的时间与资源；但当个性化展示被滥用或者违法违规使用，例如用于网络诈骗、无止境地推送商业广告，也会给公众带来负面影响。

面对发展迅速，形形色色的个性化推送、个性化展示，公众如何感受到安全与可控?App在提供个性化展示功能时，用户是否有选择甚至拒绝的权利?

本章将从个性化展示的常见类型、应用情况、主要特点等方面对个性化展示在不同领域的应用进行介绍。

（一）电商类

在电商场景下，利用用户画像向用户定向投放商品广告已经是各大电商平台重要的交易量来源。例如，根据阿里巴巴公布的数据，2018年双11主会场的跳失率从原来的50%降到了10%，基于个性化展示带来的流量，已经超过了搜索带来的流量。[1]2019年的双11，更是产生了453亿次AI个性化展示，可见个性化展示数量之巨。[2]

通常商家对于用户画像的维度可能涉及：性别、年龄、职业、地区、社交关系等方面的个人基本信息，也可能包括通过购买、浏览、收藏、评论等用户与平台交互行为所收集的身体健康信息、饮食习惯、收入水平、家庭成员状况、兴趣爱好等更为敏感的个人信息。个性化展示的具体表现形式，可以像阿里平台的“猜你喜欢”等单独展示的板块，也可以表现为对用户搜索的信息按个人兴趣与喜好进行不同排列顺序的推荐等。

由于商家对用户画像的处理越来越精细，电商向用户推荐的商品和/或服务也更为精准，节省了用户在海量商品中选购理想商品的时间，同时也提升了店铺的转化率和盈利水平。但是，这不可避免会造成用户个人信息收集、使用程度超出必要性、商家的供应商或关联方违法向其他第三方提供用户个人信息进行获利的问题。

[1]参见http://www.iwshang.com/Post/Default/Index/pid/243486.html，最后访问于2020年9月18日。
[2]参见http://www.sohu.com/a/274696022_100191067，最后访问于2020年9月18日。

（二）短视频类

在短视频场景下，短视频平台对用户画像的维度通常会涉及：性别、年龄、职业、地区等个人基本信息。同时，也会根据用户操作行为和与平台的交互，如收集浏览、完成视频浏览、中止视频浏览、关注、分享、点赞、评论、搜索、打赏等个人信息，识别用户的兴趣爱好等。

由于平台对用户进行画像分析，短视频平台向用户推荐可能喜欢的短视频能够更切中用户的兴趣点，从而使得用户获得更愉悦的视频浏览体验，给平台带来更多的用户流量，在平台上发布相关视频的所有者也能更有效地传递自己希望传递的信息资讯。但是，另一方面，用户同样面临个人信息收集程度加剧，个人信息安全保护、个人信息合法合规使用风险增加的问题。尤其是，在短视频场景下往往还涉及到人脸、声音等敏感生物识别信息的收集使用，因此风险程度可能更高。

（三）新闻资讯类

在新闻资讯类场景下，新闻资讯服务提供商主动收集用户基础个人信息的情况相比电商、短视频类少得多（如涉及地区等），更多可能是依赖于用户的搜索行为、历史浏览行为、阅读行为、时长、点赞、互动、分享等与新闻资讯服务提供商的交互操作等信息，来判断用户的兴趣偏好和对新闻资讯的感兴趣程度。同时，新闻资讯服务提供商还会根据新闻资讯内容的类似程度、用户交互行为的类似程度作为推送相关信息的依据等。

新闻资讯服务提供商提供个性化展示服务，一方面能够帮助用户更快地找到自己感兴趣的资讯，同时，也能帮助用户更迅速地在自媒体时代的海量信息中聚合、筛选出准确的、对自身有用的信息；另一方面，个性化展示服务还能保证新闻资讯服务提供商能最大化地去理解和猜测用户的兴趣，结合这些兴趣为其推荐相关资讯，提升新闻资讯的点击率。

虽然新闻资讯服务提供商收集用户的基础个人信息不多，但是如果服务商有可能采取结合其他途径收集用户的个人信息进行匹配判断，用户面临的个人信息泄露或个人信息被不当使用的风险仍不可忽视。

（四）金融服务类

在金融服务类场景下，金融机构收集用户个人信息的目的既在于维护金融交易的安全性，也在于利用相关个人信息向用户展示个性化的产品和/或服务。

一般情况下，金融机构收集的用户个人信息较多，并且大多都涉及敏感信息或重要数据，例如身份证号、人脸识别信息、个人资产及账户交易数据等金融数据。但是，发展至今，有些金融机构收集的个人信息可能已经超越了开展纯金融业务所收集的信息，其逐步通过和电商平台、社交软件（如微信、支付宝等）合作以及金融集团（或金融机构）内部共享等方式进行数据整合[3]，收集金融消费者的购物爱好、兴趣爱好、社交数据等，以求更精确全面地反映消费者的需求。

金融机构提供个性化展示的好处在于，一方面通过获取用户个人信息，能更准确地识别用户的差异化需求和特征（例如用户属于保守型、稳健性、还是激进型投资者；又如用户需要办理的业务是理财、借贷、办卡还是储蓄等），以便向用户推荐更适合的金融产品，或者根据用户特征开发更适合用户的金融产品。另一方面，对于金融机构而言，定向推送金融产品，能提升获客的命中率；也更能够利于金融机构更主动地维系客户关系；同时，利用智能算法将获客步骤前移，改变了传统的线下物理网点和一对一获客的模式，大大节省了金融机构的人力成本，这些对于传统模式的金融行业来说，可能都是重大的变革。[4]

当然，由于金融机构收集个人信息具有高度敏感性、重要性，并且采集量巨大，一旦这些信息泄露或被非法使用，对个人信息主体造成的权益损害可能都是难以估量的。现实环境中，个人信息主体对其个人信息被侵害以及被侵害的程度往往很难充分知晓，也很难及时主张自己的权益。因此，金融机构作为采集和使用个人（敏感）信息的控制者，在提供个性化展示服务时需要有更为强大的技术保障来维护个人信息的安全。

---

[3] https://mp.weixin.qq.com/s?__biz=MzU3NzQ4NTMyMg==&mid=2247483653&idx=1&sn=2975f783d3b9282814025a505d325a22&chksm=fd02ae60ca752776bd11ad11d40c6f7727570f27eabb782c33f3cd1308c35608f14f9bc3a3e3&mpshare=1&scene=1&srcid=0918TA9oFRVU9xiRoFa9uGPq&sharer_sharetime=1600422068720&sharer_shareid=c63bccca126c9be7218c26097e767d3e&key=98afdbf20ac9b6e81dffacc302b1c4997cd0e2a1cfcd00ce04eb7b09413529b2a88e89c12b6205bf4aa8e4144c6f343154d663b28df54505642cffb7dfc09b6397474ec55cfc79f56c23e2fe98fc7a51d77d34b17b1280e2420c3b1cdc2b90b39c071a51be86e0027d4c8fb7904db4e964d125bcbf86a30f9702145b7b5dffc3&ascene=1&uin=MTM5MjI1MjMwMQ%3D%3D&devicetype=Windows+10+x64&version=62090529&lang=zh_CN&exportkey=ASqGx23c6DjdnN1JNKVidJc%3D&pass_ticket=0YKP0wkZTOEpBGwXFs9A4rqkwrfJx5p%2BithNsvuoFZ74z0Mj3%2BARL8kICA8o91FF&wx_header=0，最后访问于2020年9月18日。

[4] 参见http://www.woshipm.com/user-research/522624.html，最后访问于2020年9月18日。

（五）外卖类

在外卖类场景下，外卖平台收集用户个人信息的维度通常包括性别、年龄、职业、地区等，平台同时也会收集用户的行为数据，包括其下单历史、喜好、评价、消费水平、投诉和客服反馈等。在对商家进行识别和分类的基础上，外卖平台通常根据用户的喜好生成展示给每个用户不同的外卖商家排名，优先展示用户经常购买、收藏、或价格及品类相近的商家，而用户投诉、差评过多的商家就会被靠后展示。以饿了么为例，平台 90% 以上的用户在下单前进行决策，通过各式搜索推荐选择下单的商家与菜品。依赖搜索排名实现个性化服务，这是外卖平台提供个性化服务与其他场景的不同之处。[5]

此外，外卖平台通常将时间分为早餐、午餐、晚餐、夜宵四个时间段，通过对商家主营类目的识别和分类，每个时间段展示不同的商家和商家排名（如早餐时段更多地曝光提供早餐的商家），也能够缩短用户进行搜索和选择的路径。平台还可能根据商家所在的不同区域，按照订单量和评价的分类，向用户展示不同的商家和商家排名。

外卖类场景与其他场景显著不同之处，还在于有较强的时间性。平台在集中的上述四个时间段内需要处理大量的需求，建立有效的个性化展示系统，可以从流量分发的角度调控峰值订单。通过分析用户的客观画像（包括配送距离、用餐时间等）和主观上对配送时间的敏感程度（历史订单、投诉和好评记录等），调配餐厅、物流、配送人员和运营人员等资源，能够有效节省用户时间，满足用户的不同需求，提升用户的使用体验和满意度。

[5]参见https://blog.csdn.net/weixin_33719619/article/details/89092077，最后访问于2020年9月18日。

二、个性化展示的法律规制

（一）法律法规

就个性化展示来说，目前我国呈现出分散式立法的特点，尚无专门针对个人信息保护的统一立法，也没有关于个性化展示这一主题的专门立法。总体上，目前立法对电子商务和新闻资讯两种场景进行了特殊规定，因此，这些场景就需要满足特殊规定。对于个性化展示的一般规定则适用于所有场景，相关规定如下：

1. 电商场景

我国在涉及电商场景下个性化展示/推送方面的规定主要包括《电子商务法》《消费者权益保护法》《网络安全法》《互联网广告管理暂行办法》《电信和互联网个人信息保护规定》《信息安全技术　个人信息安全规范（GB/T　35273-2020）》（以下简称“《个人信息安全规范》”）《网络交易监督管理办法（征求意见稿）》《数据安全管理办法（征求意见稿）》等。

《电子商务法》第十八条规定，电子商务经营者在根据兴趣爱好、消费习惯等特征向消费者提供商品或者服务的搜索结果时，应当向消费者提供不针对其个人特征的选项。《网络交易监督管理办法（征求意见稿）》第十九条和《个人信息安全规范》第7.5条b）款进行了相同的规定。《互联网广告管理暂行办法》第十三条规定，对于通过程序化购买广告方式发布的互联网广告，互联网广告的发布者和广告经营者应当清晰标明广告来源。根据《消费者权益保护法》第九条，消费者有权自主选择商品或服务，有权进行比较、鉴别和挑选。《数据安全管理办法（征求意见稿）》第二十三条规定，网络运营者利用用户数据和算法推送商业广告时，应当标注“定推”字样。由此，为保障消费者的知情权，个性化广告应当以显著方式对商品进行标识，同时需要提供针对非针对用户个性化广告的商品，以便消费者可以进行比较和挑选。

此外，由于个性化展示/推送主要基于潜在消费者的兴趣爱好、消费习惯等个人信息向消费者推送商业广告，因此也需要满足我国《网络安全法》第四十一条、《个人信息安全规范》等关于收集、使用个人信息的相关规定，遵循合法、正当、必要、透明的原则，公开展示隐私政策，并征得个人信息主体的同意。

在电商场景中，通常还会利用用户画像向用户定向投放个性化广告并进行推送。个性化广告主要是利用用户个人网络浏览历史、兴趣偏好等信息开展精准营销、推送个性化商业广告。“程序化广告”便是实现上述目的的主要方式之一。程序化广告是一种通过信息技术自动完成广告采买及广告投放过程的互联网广告投放形式，其集合了媒介资源方、广告主和广告需求方平台，由媒介资源方（信息提供者）通过分析用户在平台的使用、购买、浏览偏好信息与广告主体互通有无，从而为广告主达到广告的精准投放。个性化广告以实现广告精准投放为目标，凭借其绝对的经济优势和技术优势成为电子商务经营者利用大数据进行营销的重要手段。

因此，我国企业也制定了专门针对个性化广告方面的行业规则来指导实践。2014年3月15日，我国第一部规范互联网个性化广告的行业标准《中国互联网定向广告用户信息保护行业框架》（以下简称“《框架标准》”）正式发布并实施，新浪、腾讯、百度、中国电信等首批签署了该标准。《框架标准》充分强调了保障用户知情同意、要求实现用户对信息的控制等，和成文法规的规定基本一致。值得一提的是，目前关于数字广告应用与安全技术要求方面的国家标准也正在制定中，我们可以继续观察未来的进一步行业实践动向。

2. 新闻资讯场景

中央网信办、工信部、公安部、市场监管总局《关于开展App违法违规收集使用个人信息专项治理的公告》要求App运营者收集使用个人信息时要严格履行《网络安全法》规定的责任义务，对获取的个人信息安全负责，采取有效措施加强个人信息保护。遵循合法、正当、必要的原则，不收集与所提供服务无关的个人信息；收集个人信息时要以通俗易懂、简单明了的方式展示个人信息收集使用规则，并经个人信息主体自主选择同意；不以默认、捆绑、停止安装使用等手段变相强迫用户授权，不得违反法律法规和与用户的约定收集使用个人信息。倡导App运营者在定向推送新闻、时政、广告时，为用户提供拒绝接收定向推送的选项。

《个人信息安全规范》第7.5条c）款特别规定了新闻资讯服务场景下的个性化展示合规要求。根据该款，个人信息控制者应当向信息主体提供简单直观的退出或关闭机制，如信息主体选择退出或关闭，则应当向个人信息主体提供将相关个人信息进行删除或匿名化处理的选项。

3. 个性化展示的一般规定

自2019年来《个人信息安全规范》经历了多次修订。截至目前，《个人信息安全规范》确立了专门针对用户画像和个性化展示的条款，并对用户画像进行了定义，并区分了直接用户画像和间接用户画像的概念。

同时，《个人信息安全规范》第7.4条规定了用户画像的使用限制。根据该条a）款，用户画像中对于个人信息主体的特定特征描述不应当包含淫秽、色情，赌博等违法违规内容。该条b）款规定，使用用户画像不应当侵害公民合法权益，也不得危害国家利益。该条c）款则规定，在使用个人信息时尽量避免精确定位到个人，并建议在推送广告时，最好使用间接用户画像。[6]

根据本报告附录「相关定义列表」可见，“个性化展示”与“个性化广告”概念的分野在于推送内容的差异。后者倾向于为满足特定营销目的而直接或者间接地向用户推送与商品或者服务相关的商业广告；而前者推送的内容既可能包括广告，也可能包括其他信息内容及任何呈现在用户面前的内容，例如新闻资讯、文章、视频等等。据此，个性化广告可能不仅需要满足与其相关的特殊要求，还需要满足与我国与个性化展示相关的一般性法律规定。

针对个性化展示的问题，如前所述，《个人信息安全规范》第7.5条b）款和c）款特别规定了电子商务场景和新闻资讯信息服务场景下的个性化展示。而a）款和d）款则适用于所有场景的个性化展示：a）款要求个人信息控制者至少做到对个性化展示的内容和非个性化展示的内容进行区分。区分的方式既可以采用标明“定推”的方式，也可以通过不同的栏目、板块、页面进行分别展示；d）款则建议个人信息控制者建立个人信息主体的自主控制机制，保障个人信息主体能够对个性化展示的程度进行调控。

需要注意的是，《个人信息安全规范》第7.7条要求个人信息控制者在仅依据信息系统自动决策而做出显著影响信息主体权益的决定时，必须向信息主体提供投诉渠道。通过反映到隐私政策或个人信息保护政策来说，根据《个人信息安全规范》第5.5条，隐私政策中必须明确对信息系统自动决策进行投诉的方法。《个人信息安全规范》第7.7条还规定了对于信息系统自动决策的额外要求，即需要进行事前和事中（定期）的个人信息安全影响评估。

[6]根据《个人信息安全规范》第3.8条，直接使用特定自然人的个人信息，形成该自然人的特征模型，称为直接用户画像。使用来源于特定自然人以外的个人信息，如其所在群体的数据，形成该自然人的特征模型，称为间接用户画像。

除了《个人信息安全规范》上述要求外，公安部网络安全保卫局、北京网络行业协会、公安部第三研究所《互联网个人信息安全保护指南》中规定，完全依靠自动化处理的用户画像技术应用于精准营销、搜索结果排序、个性化推送新闻、定向投放广告等增值应用，可事先不经用户明确授权，但应确保用户有反对或者拒绝的权利；如应用于征信服务、行政司法决策等可能对用户带来法律后果的增值应用，或跨网络运营者使用，应经用户明确授权方可使用其数据。中国互联网协会《用户个人信息收集使用自律公约》第九条规定，使用个性化展示新闻信息服务的，应为用户提供简单直观的退出或关闭个性化展示模式的选项或者不基于用户个人信息的新闻推荐选项。据用户爱好、消费习惯等特征向其个性化展示商品或服务的搜索结果的，应当同时向用户提供不针对个人特征的选项。基于用户所选择的特定位置进行展示和排序搜索结果的除外。

综上所述，在个性化展示方面，目前的法律法规侧重于保护用户的知情权和自主选择权，要求征得用户同意，并保证用户对其个人信息可以得到控制。总结如下：(1) 通过要求以不同的标识对个性化展示的内容和非个性化展示的内容进行区分，从而保障用户的充分知情权；(2) 由于个性化展示以收集、使用与用户兴趣爱好、浏览记录等个人信息为基础，这就要求企业在隐私政策中向用户告知个人信息的收集会被用于用户画像和个性化展示，并征得用户的同意；(3) 要求企业向用户提供自主控制机制，例如提供不针对用户特定个人特征的选项、提供直观的关闭和退出选项、在用户选择退出后对相关个人信息进行删除、提供相应的投诉机制、建立相关标签、画像维度的自主调控机制等，来保障用户对其个人信息的自主可控。

（二）监管动态

个人信息收集、使用的问题已成为监管部门整治工作中的重中之重。自2019年1月中共中央网络安全和信息化委员会办公室、工信部、公安部、国家市场监督管理总局联合发布《关于开展App违法违规收集使用个人信息专项治理的公告》以来，个人信息相关的监管在2020年更是进入了深水区。个性化展示也成为其中一项整治内容。

2019年11月6日，工信部发布《关于开展App侵犯用户权益专项整治工作的通知》，将重点对四个方面8类问题开展规范整治工作，其中在“违规使用用户个人信息方面”，将“强制用户使用定向推送”列为一类重要问题。

根据2019年11月28日发布的《App违法违规收集使用个人信息行为认定方法》，利用用户信息和算法定向推送信息，如未向用户提供非定向推送信息的选项，则属于“未经用户同意收集使用个人信息”。同时也规定，不得仅以定向推送信息为由，强制要求用户同意　　收集个人信息。此外，2020年3月，信安标委发布的《网络安全标准实践指南——移动互联网应用程序（App）收集使用个人信息自评估指南》（征求意见稿）针对个性化展示的规定与制约，与《App违法违规收集使用个人信息行为认定方法》并无出入。2020年7月28日，《工信部关于开展纵深推进App侵害用户权益专项整治行动的通知》中明确，App、SDK不得强制用户使用定向推送功能。重点整治App、SDK未以显著方式标示且未经用户同意，将收集到的用户搜索、浏览记录、使用习惯等个人信息，用于定向推送或广告精准营销，且未提供关闭该功能选项的行为。

因此，监管部门已经将重点关注到App在进行个性化展示时，是否向用户告知或以显著方式标示，以及是否为用户提供了关闭该功能的选项。特别是针对有些App使用个性化展示的功能，有些企业虽然也在其隐私政策中进行了披露，但未在产品界面上设计提示退出或者关闭个性化展示模式的选项或按钮（如拒绝接受定向推送信息，或停止、退出、关闭相应功能的机制），需要高度重视并积极探讨改进方案。

三、常见应用的个性化展示情况测评

为了更直观地展示我国个性化展示技术运用的现状，南都个人信息保护研究中心（以下简称“南都”）以常见的移动应用（App）为例，从保证用户自主控制与选择权的初衷出发，测评了当前市面上20款常用App使用个性化展示对用户友好的情况。本节通过测评对象、标准、过程和测评结果分析等具体描述，向大家介绍目前相关行业对上述所提及的法规遵守与落实的基本情况。

需要特别说明的是，本次测评仅从中立第三方、普通用户使用App的角度，测试相关App是否保障用户对其使用个性化展示享有充分的知情权与控制权。鉴于测评范围的局限性，本次测评不对测评对象App的整体合规性作出评价。

（一）测评方法

1. 测评对象

本次测评的对象为以下20款常用App，类别包括电商、资讯、短视频、生活服务。

图1：20款被测App及类型

2. 测评标准

本次测评标准的制定依据包括《中华人民共和国广告法》、《数据安全管理办法（征求意见稿）》、《个人信息安全规范》等法律法规或国家标准，并综合考虑各项标准的重要性和可操作性给予一定的权重，总分为100分。

需要注意的是，以上测评标准的依据，由于部分法律法规或国家标准仍然处于征求意见稿阶段，并非已生效，且测评标准的权重无法完全避免对测评要点重要性、实施难度、实施层次多少等的主观理解，因此本次测试结果仅作为中立第三方的评价，供读者参考。

具体标准	分值	测评要点
1. App 开发者在向用户提供业务功能的过程中使用个性化展示的，应显著区分个性化展示的内容和非个性化展示的内容。	20	标明“定推”等字样，或通过不同的栏目、版块、页面分别展示等，可得 25 分；没有标明不得分。
2. App 开发者在隐私政策中明确告知个性化展示的目的及收集的个人信息 。	15	详尽描述向用户推送的目的、方式、使用了哪些信息等内容，可得 15 分；简单提及，可得 5 分；未提及不得分。
3. App 开发者在隐私政策中明确告知关闭/退出个性化展示的路径。	10	明确告知，可得 10 分；未明确告知不得分。
4. App 开发者在隐私政策中承诺用户关闭/退出个性化展示后，不再处理相关个人信息。	15	在隐私政策中做出相关承诺可得 15 分；没有相关承诺不得分。
5. App 开发者为用户提供关闭/退出个性化展示的选项。	20	提供选项，可得 20 分；提供选项但需重复关闭/退出，可得 10 分；未提供不得分。
6. App 开发者设置用户对标签的自主控制机制。	20	有可编辑、可删除的个人化标签管理系统可得 20 分；若仅可编辑、删除根据个人生成的系统预设标签，可得 15 分；仅有固定的系统预设标签或仅有单个广告的用户反馈机制，可得 5 分。

3. 评估样本采集

（1）采集设备

安卓移动端：安卓移动端是指华为、三星、Vivo等常用安卓应用市场。

（2）采集时间

本次测评取证采集时间为2020年9月1日至17日。该时间段以外的修改不计入测评。

（3）采集内容

视频资料：使用手机录屏软件等对整个采集过程进行全程录像。

图片资料：对隐私政策、个性化展示相关页面进行截图，以便后期查阅、评分以及作为证据使用。

（二）测评结果分析

1. 总体情况

按照总分，20款App可划分为四个等级，用户友好程度高（90分以上）、用户友好程度较高（76-90分）、用户友好程度中等（61-75分）、用户友好程度低（60分及以下）。

测评得分

App	得分
淘宝	85
美团	85
考拉海购	85
苏宁易购	85
快手	75
今日头条	75
拼多多	75
京东	75
聚美优品	65
抖音	65
知乎	65
小红书	65
蘑菇街	60
唯品会	60
饿了么	55
飞猪	55
携程	45
微信	40
大众点评	40
新浪微博	35

图2：20款App得分情况（分数从高到低排序）

从整体测评情况来看，20款被测App个性化展示的合规程度集中在中等及以下。其中合规程度高的App个数为零；合规程度较高的App有四款，分别为淘宝、美团、考拉海购和苏宁易购；合规程度中等和低的App各有八款，占总数的80%。

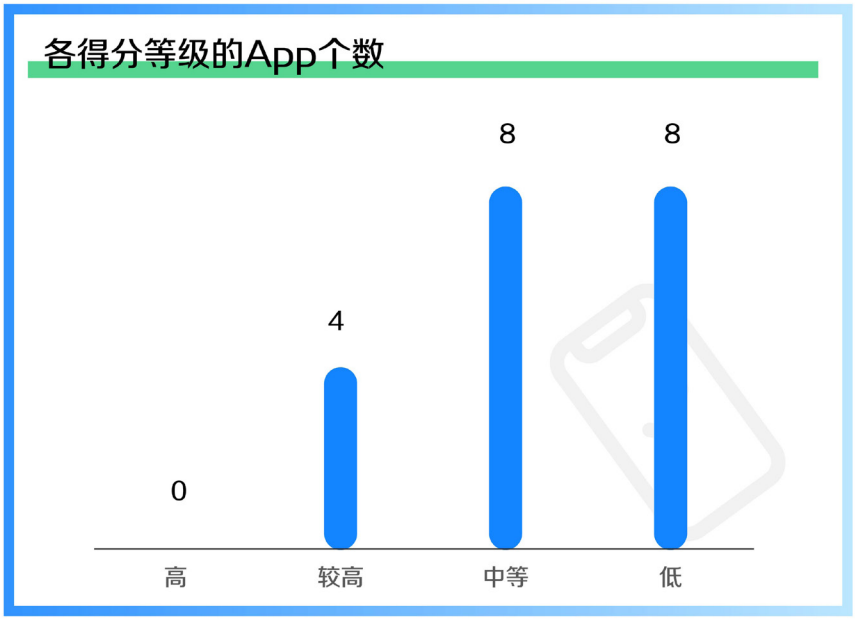


图3：20款App合规程度分布

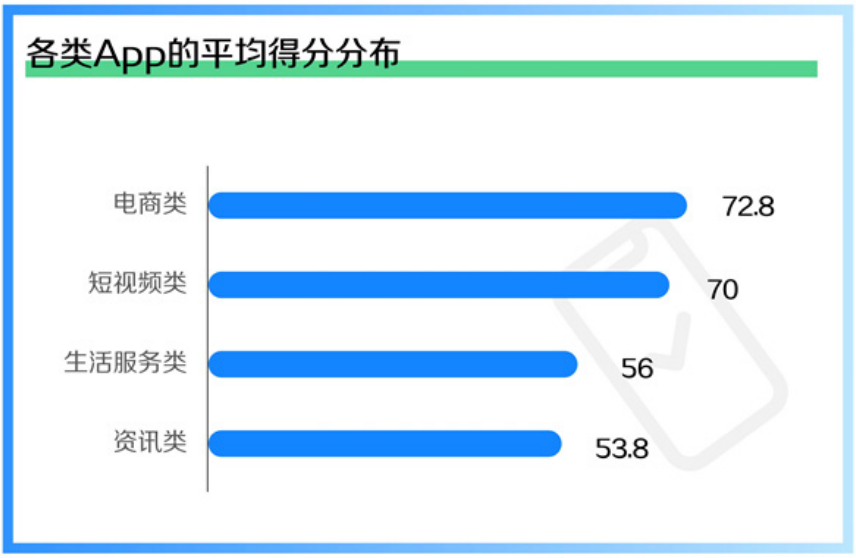


图4：各类App的平均得分分布

2. 具体项分析

从整体来看，在绝大多数测评项中，得到满分的App占比都能达到75%及以上，其中“明确告知个性化展示的目的及收集的个人信息”项符合要求的比例最高。

而主要的失分点在于两项：一是，明明在隐私政策中告知用户App提供个性化展示功能，却没有在实际使用过程中显著区分个性化展示的内容和非个性化展示的内容。

二是，不少App没有为用户提供编辑或删除个性化标签的功能，比如有的App只能对单条广告选择“不感兴趣”，不能批量编辑；而即使提供了这一功能，也只能编辑和删除系统已经设定好的标签，而非完全由个人历史数据生成的标签。

（1）个性化展示标记

根据测评结果，20款App中，仅有淘宝、美团、考拉海购、苏宁易购、飞猪等五款App通过设立单独栏目（“猜你喜欢”）来显著标明个性化展示的内容。

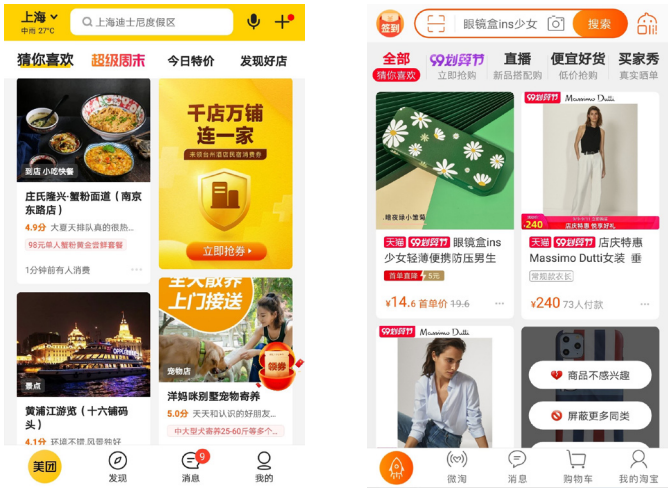


图5：淘宝（左）和美团的“猜你喜欢”栏目

南都还注意到，有的App会在类似的页面位置单设“为你推荐”栏目，但仅从字面意义难以认定是否为个性化展示的内容，没有达到显著区分个性化展示的内容和非个性化展示的内容的目的，因此会相应减分。

从上述数据不难看出，目前在标识个性化展示方面，国内头部企业App的主流做法是开设单独栏目，而非在单体广告上标注“定推”字样。

（2）隐私政策条款

i.明确告知目的及收集的个人信息

根据测评结果，20款App均在隐私政策中提及了用户画像和个性化展示机制生成的方式，其中19款较为详细地告知为了展示用户感兴趣的商品或服务信息，可能会收集订单信息、浏览信息等进行数据分析并形成用户画像。

为了将您感兴趣的商品或服务信息展示给您，或在您搜索时向您展示您可能希望找到的商品或服务，我们可能会收集您的订单信息、浏览信息、您的兴趣爱好（您可以在账户信息中填写）进行数据分析以形成用户画像。我们还可能为了提供服务及改进服务质量的合理需要而获得的您的其他信息，包括您与客服联系时您提供的相关信息，您参与问卷调查时向我们发送的问卷答复信息，以及您与我们的关联方、我们合作伙伴之间互动时我们获得的相关信息。对于从您的各种设备上收集到的信息，我们可能会将它们进行关联，以便我们能在这些设备上为您提供一致的服务。我们可能会将来自某项服务的信息与来自其他服务的信息结合起来，以便为您提供服务、个性化内容和建议。如果您不希望受个性化内容的影响，您可以在商品展示页选择按照分类进行浏览和查找商品和服务。我们还在搜索结果中向您提供了按照价格、销量排序等不针对个人特征的选项；未经您的明确同意，我们不会将您的相关个人信息提供给第三方。

图6：京东的隐私政策相关条款

唯独在该项被扣分的新浪微博，仅在隐私政策中简略提及“会使用你所提供信息在微博平台中向你展示或提供广告和促销资料，向你通告或推荐微博的服务或产品信息，以及其他此类根据你使用微博服务或产品的情况所认为你可能会感兴趣的信息”，但并未明确说明基于哪些个人信息，以及是否会形成用户画像。

个人信息的使用

为了向你提供更好的服务或产品，微博会在下述情形使用你的个人信息：
1)根据相关法律法规的要求；
2)根据你的授权；
3)根据微博相关服务条款、应用许可使用协议的约定。

此外，**你已知悉并同意：在现行法律法规允许的范围内，微博可能会将你非敏感的个人信息用于市场营销，**使用方式包括但不限于：微博会使用你所提供信息在微博平台中向你展示或提供广告和促销资料，向你通告或推荐微博的服务或产品信息，以及其他此类根据你使用微博服务或产品的情况所认为你可能会感兴趣的信息。其中也包括你在采取授权等某动作时选择分享的信息，例如当你新增好友、在动态中新增地标、使用微博的联络人汇入工具等。

图7：新浪微博的隐私政策相关条款

ii.明确告知关闭/退出路径

在提到个性化展示相关的章节中，17款App在隐私政策中明确告知了关闭/退出路径。

比如考拉海购在隐私政策中提到，用户可以通过“我的考拉-设置-系统权限设置-隐私设置”管理个性化推荐功能的开关，并明确指出，如果用户关闭个性化推荐，“猜你喜欢”和“我的考拉-为你推荐”的个性化推荐将失效。

在个性化广告方面，微信在“我们如何使用信息”章节附上了“关于广告”的页面链接，点击之后可以看到腾讯广告的工作原理、如何管理广告、广告行业标准参与情况等内容。点击“管理”，便可进入“腾讯广告个性化设置”页面，选择打开或关闭个性化推荐广告。

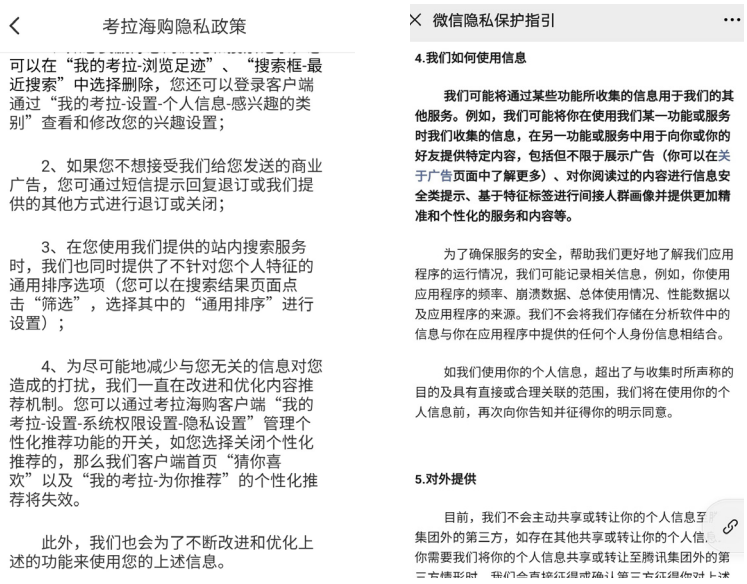


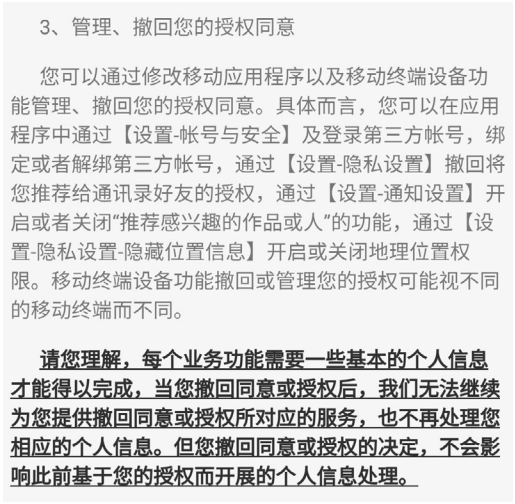
图8：考拉海购（左）和微信的个性化展示相关页面

而饿了么、大众点评、新浪微博等三款App尽管在“设置”中提供了关闭/退出选项，却并未在隐私政策中详细告知路径；飞猪则没有提供这一选项。

iii.承诺关闭/退出后不再处理个人信息

根据《个人信息安全规范》，当个人信息主体选择退出或关闭个性化展示模式时，个人信息控制者应向个人信息主体提供删除或匿名化定向推送活动所基于的个人信息的选项。

具体体现在实际测评中，个性化展示选项通常是一个开关，用户可以滑动打开和关闭，对应着选择同意和不同意。80%的App均在隐私政策中承诺，当用户撤回同意或授权，将不再处理其相应的个人信息，但用户撤回同意或授权的决定，不会影响此前基于其授权而开展的个人信息处理。



3、管理、撤回您的授权同意

您可以通过修改移动应用程序以及移动终端设备功能管理、撤回您的授权同意。具体而言，您可以在应用程序中通过【设置-帐号与安全】及登录第三方帐号，绑定或者解绑第三方帐号，通过【设置-隐私设置】撤回将您推荐给通讯录好友的授权，通过【设置-通知设置】开启或者关闭"推荐感兴趣的作品或人"的功能，通过【设置-隐私设置-隐藏位置信息】开启或关闭地理位置权限。移动终端设备功能撤回或管理您的授权可能视不同的移动终端而不同。

请您理解，每个业务功能需要一些基本的个人信息才能得以完成，当您撤回同意或授权后，我们无法继续为您提供撤回同意或授权所对应的服务，也不再处理您相应的个人信息。但您撤回同意或授权的决定，不会影响此前基于您的授权而开展的个人信息处理。

图9：快手的隐私政策相关条款

(3) 关闭/退出选项

测评结果显示，除了飞猪，其余19款App均提供了关闭/退出个性化展示的选项，而且绝大多数是"一键关闭"的形式，但入口和关闭有效期有所差异。

有的App可以通过长按商品并点击个性化相关设置选项或从隐私政策直接跳转，比如今日头条、微信；但大多数App则会把个性化展示开关放在"设置"、"隐私"等页面。

在提供开关的基础上，少数App还会制作专门页面介绍个性化展示的运行机制。比如淘宝可以通过点击"设置"-"隐私"-"我有疑问"-"如何管理我的个性化广告?"进入相关页面，了解个性化广告保护原理，并进入"隐私实验室"设置个性化广告。

该页面提到，"在关闭的有效期内，您仍然会看到广告，您看到的广告数量不会变化，但广告的相关性会降低。此外，选择关闭部分兴趣类别后，不会停止您的信息收集。但是所收集的信息不会用于向您推荐您已关闭的广告类别。"

图10：淘宝的个性化展示设置页面

值得注意的是，除了没有提供关闭/退出选项的飞猪以外，有四款App均为这一选项设置了“有效期”，短则三个月，如新浪微博；长则六个月，如淘宝、微信和大众点评。也就是说，三个月或六个月后，用户需要再次手动关闭个性化展示。

图11：新浪微博（左）和大众点评的个性化展示关闭/退出页面

据媒体报道，这种设置关闭有效期的做法曾引发公众对于关闭程序化广告“怎么这么难”的质疑。对此，南都认为，当用户明确拒绝个性化展示功能时，App无权代替用户做出撤回授权的动作，因此上述四款App在该项仅得到一半分数。

其余15款App则未设置时限，意味着一旦用户选择关闭个性化展示，将被视为永久关闭。此外，所有19款提供了关闭/推出个性化展示开关的App均将其设为默认开启。

（4）编辑或删除已有标签

根据《个人信息安全规范》的要求，App宜建立用户对个性化展示所依赖的个人信息（如标签、画像维度等）的自主控制机制。

从进入标签编辑页面的入口看，有的App可以通过点击搜索页面的相关功能键进行跳转，比如今日头条、快手可以点击“为什么看到此广告”、“设置感兴趣的广告”直接跳转至广告管理或标签管理页面；有的则需要经由“设置”-“常见问题”进入。

图12：今日头条进入标签管理页面路径

结合大部分App的现实操作情况和国外优秀案例，我们将对标签的自主控制机制转换为两种做法，一是设置可编辑、可删除的个人化标签管理系统，二是仅有固定的系统预设标签或单个广告的用户反馈机制，其中单个广告的用户反馈机制是指长按广告或点击关闭按钮弹出的功能页面，用户可以选择“不感兴趣”、“不喜欢”做出反馈。

测评结果显示，淘宝、快手、今日头条、拼多多、新浪微博等五款App设有可编辑、可删除的统一标签管理系统，尽管是系统预设好的标签，但会根据不同用户的使用习惯形成不同的标签池；12款App提供了对单个广告的用户反馈机制，其中考拉海购和聚美优品同时也提供了固定的系统预设标签供用户选择；剩余三款App则没有对标签的自主控制机制。

统一标签管理系统通常需要经过个性化展示的设置页面进入。App会提供一些系统设定的标签供用户选择，比如女装、鞋包、海淘、二次元爱好、穿搭达人等等。

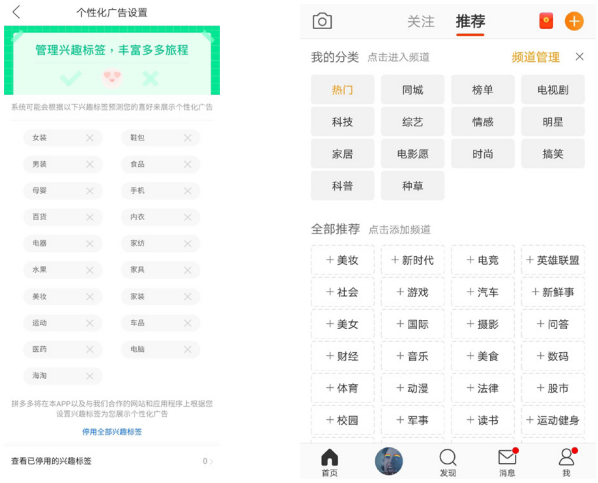


图13：拼多多（左）和新浪微博的标签管理系统

不难看出，这些标签都是App“定制”好的，整体的设计类似于了解用户的偏好，而不是直接根据用户的个人特点和使用习惯生成的。用户的偏好与系统设定的标签完全吻合的情况除外。

而与之相对的，是考拉海购和聚美优品提供的固定的系统预设标签，比如考拉海购在“设置”-“个人信息”页面设有“感兴趣的类别”一栏，用户可以从12个兴趣类别中选择，至少选一项；聚美优品同样提供了12个分类，用户可至少选择三个。相比上述五款的标签池，这两款App提供的标签都非常笼统，如“彩妆”、“视频”、“配饰”等，而且需要用户手动勾选标签，后台不会直接代为添加。

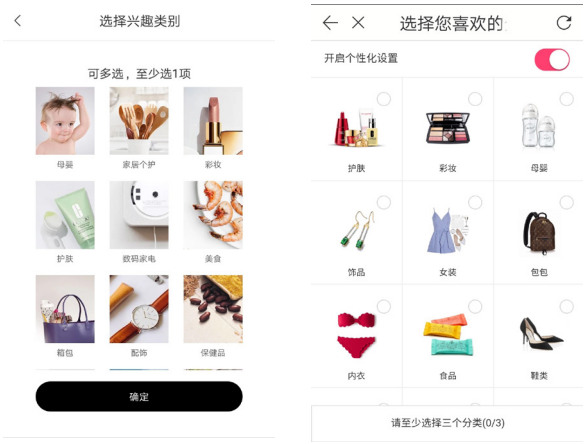


图14：考拉海购（左）和聚美优品的标签管理系统

单个广告的用户反馈机制则如长按抖音“推荐”页面中的视频，会跳出标有“转发”、“收藏”、“不感兴趣”和“保存本地”四个选项的弹窗，用户可以点击“不感兴趣”来减少相关推送，实现对后台标签的自主控制。类似的，点击知乎广告的关闭按钮，用户可以做出“看过了”、“内容不感兴趣”等反馈。

图15：抖音（左）和知乎的单个广告反馈机制

四、个性化展示主要问题及分析

（一）法律层面：术语零散不统一

我国2020年10月生效的《个人信息安全规范》、2019年发布的《数据安全管理办法（征求意见稿）》、2016年发布的《互联网广告暂行办法》等法律法规或国家标准使用了定向推送、个性化展示、个性化推送、程序化（购买）广告[7]等多个不同的概念。通常意义上，我们理解，这些概述并非法律术语，而是根据一系列利用用户个人信息并对其进行针对性处理的行为指称。

特别的是，《个人信息安全规范》第7.5条a）款要求所有个人信息控制者在向个人信息主体提供业务功能的过程中使用个性化展示的，应显著区分个性化展示的内容和非个性化展示的内容，区分方式包括标明“定推”等字样，或通过不同的栏目、版块、页面分别展示等。根据该条b）款，在电子商务场景下提供个性化展示的，应当同时向消费者提供不针对其个人特征的选项。根据该条c）款，在新闻资讯信息服务场景中，则应当为个人信息主体提供简单直观的退出或关闭个性化展示模式的选项；同时，当个人信息主体选择退出或关闭个性化展示模式时，应当向个人信息主体提供删除或匿名化定向推送活动所基于的个人信息的选项。又如，《数据安全管理办法（征求意见稿）》第23条规定，网络运营者利用用户数据和算法推送新闻资讯信息、商业广告等，应当以明显方式标明“定推”字样等。

以上条款中，个性化推送、个性化展示、定推、定向推送的概念在同一规范或者不同法规之间被相互替代使用，从所表达的意思进行推断，这些概念在我国语境下的本质含义可能差别不明显。此外，我们观察到，2019年6月21日发布的《个人信息安全规范》（征求意见稿）第7.5条还同时使用个性化推送、个性化展示两个概念，将向个人信息主体提供个性化业务功能、电子商务服务、以及推送个性化新闻资讯等过程中发生的个性化服务，统称为“个性化展示”，这在某种程度上印证了我们的上述推测。

进一步来讲，以上这些概念所指的行为，一般来说可以拆解为两大步骤：（1）通过一定的自动化、非自动化技术，对个人信息主体特征进行分析，如个人信息主体的工作表现、生活习惯、购物偏好等，形成关于该个人信息主体的标签和画像；（2）为了商业或非商业目的，利用对个人信息主体标签或画像分析的结果，对个人信息主体进行千人千面的展示、定向推送或者推荐相关的产品和/或服务。通常个性化展示、个性化/定向推送等行为既可

[7]《互联网广告管理暂行办法》第13条规定，互联网广告可以以程序化购买广告的方式，通过广告需求方平台、媒介方平台以及广告信息交换平台等所提供的信息整合、数据分析等服务进行有针对性地发布。

能是商业性质，也可能是非商业性质的；而程序化（购买）广告概念涵盖的实则就是商业性质的广告推广行为。虽然在阶段（2）出于不同的目的可能对应不同的名词以及行为外观，但就阶段（1）的画像阶段，定向推送、个性化推送、个性化展示、程序化（购买）广告等这些概念从本质上都需要包括对个人信息主体进行画像分析这一共性的要求。至于利用用户画像所从事推送、展示等，其中的差异较为有限，最多可能是根据不同行业的表达习惯或者触达到用户的感觉不同而作的区分。

另外，可能还应当注意利用用户画像所从事的行为是否赋予用户以选择权，而分为两类展示/推送的结果：（1）网络服务提供者根据用户画像向用户提供相关产品和/或服务，供用户进行选择；（2）网络服务提供者根据用户画像，直接区分地向消费者提供符合其标签的服务。两者的差异在于，前者用户接收到提供的产品和/或服务后仍享有选择权，而后者用户只能被动接受，并无选择的机会。例如，电商场景下，电商平台可能会从消费者以往在平台购物的情况而判断出顾客的购物习惯，顾客再次登录购物平台时，平台会根据顾客的购物习惯自动跳出展示类似物品的弹窗，此时顾客可以选择购买推荐的商品也可选择不购买。游戏场景下，平台会通过儿童在注册游戏平台账户时填写的年龄赋予该账户以儿童的标签，当该用户再次登录时，平台可依据标签向该账号的用户提供区别于一般服务的儿童特殊服务，如不开放消费功能、定时强制休息等，此时儿童并无选择是否接受儿童特殊服务的机会，只能被动接受平台根据标签所推送的内容。但是，我国目前的法律法规或国家标准并未对此种区分作出回应。

综上，尽管我国法律法规与国家标准中仍存在术语表达不一致的情况，但未来我国立法是否会对上述概念进行统一（或者说，是否可以给予相对较清晰的定义，以避免普通用户在理解上发生分歧），这一点有待我们进一步观察。

（二）技术层面：难以删除或进行匿名化处理

1. 个性化推送的关键技术——用户画像

个性化展示依赖于用户画像技术，用户画像越精准，推送的内容或商品越精准。同时，个性化展示只是用户画像的一个应用场景，在产品设计与功能迭代升级、市场经营策略、广告精准投放等方面，用户画像也发挥着十分重要的作用。

用户画像的核心工作是给用户打上各种类型的标签。一套面向应用目标、合理的标签体系是决定用户画像成功与否的关键因素之一。在建立标签体系的过程中，需要使用信息

检索、统计学、机器学习、自然语言处理（NLP）等技术。在底层技术方面，Hadoop的HDFS分布式文件系统、Spark和Rhadoop计算框架、MangoDB数据库等在用户画像工具中得到广泛应用。这些大数据相关技术，能够提升数据汇聚、处理能力，实现更为复杂的算法，一方面可以给用户打上更多维度、更多层次的标签，一方面可以预测用户的属性和行为。

用户画像的标签体系一般都是层次化的，而且标签体系也是逐层构建起来的。从底层向上，通常可以分为事实标签、模型标签、预测标签。其中，只有事实标签是基于原始数据，经过简单统计分析形成的。模型标签、预测标签是对下层标签进行数据建模分析，利用机器学习、自然语言处理等技术，进行构造的。原始数据的来源可以非常广泛，以新闻资讯信息服务为例，包括用户注册信息（用户主动提交的信息）、用户设备信息等用户基本信息，用户浏览的新闻链接、阅读时长、转发、评论、点赞等用户行为信息，用户登录日志等日志信息，地理位置信息等，以及可能来自其他业务线条或第三方的用户消费数据、交易数据等。

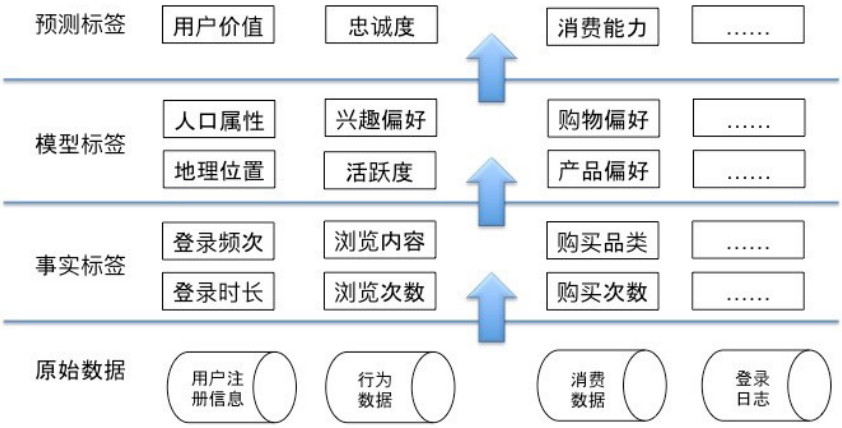


图16：用户画像的标签体系示意图

在用户画像过程中，可能由于缺少原始数据的支持，无法直接对某个用户生成标签。这时，可以通过构建标签扩散模型，将一个群体的标签传递给与其行为相似的其他用户。还是以新闻资讯信息服务为例，用户在使用网站、App等新闻资讯信息服务时，不太倾向于告诉新闻资讯信息服务提供者自己的性别，即使在注册页面有性别的填写项，实际填写的比例和准确率也未必理想。基于男性和女性在新闻浏览行为方面存在差异的事实基础，为了实现对全量用户的性别画像，可以将已知性别用户的行为数据作为训练数据，使用LR、线性SVM等模型进行训练，然后用这个经过训练的模型，分析那些无性别标签的用户行为数据，就能够预测这部分用户的性别，实现用户性别打标。

2. 个性化展示在技术领域面临的问题

从用户画像的实现原理可以得出结论：普通用户几乎没有能力阻止企业对其画像，除非永久性的停止使用产品或服务；企业向用户提供退出个性化展示的选项，区分个性化展示内容和非个性化展示内容，没有明显的技术实现困难——企业面临的真正困难是用户选择或退出个性化展示模式时，删除或匿名化定向推送活动所基于的个人信息。如前所述，用户画像实际上是对用户构建一个数学模型，利用标签高度精炼地描述用户特征。个性化展示是基于用户标签的推送，从前述用户画像标签体系的构建方法可以看出，不是所有的用户标签都是通过处理用户个人信息直接生成的，里面还包括运算、推导、建模的过程，加之机器学习等技术的应用，从个性化展示活动到确定使用了哪些用户标签，再到确定标签生成过程中使用了哪些用户个人信息，是有相当技术复杂度的。即使对于科技实力雄厚的大型互联网企业，能够在技术上实现删除或匿名化个性化展示活动所基于的个人信息，也是需要付出相当的经济和人力成本的。

（三）企业合规层面：未能履行个人信息处理的相关要求

个性化展示是网络技术普及与发展的产物，本身是一种中立性的技术，没有好坏之分。如果网络服务提供者能够合法、合理地使用该技术，很大程度上就能够趋利避害，发挥其精准化、高效率的益处。反之，如果在运用的过程中，没有法律的规制，或者不遵守法律或国家标准的规范化要求，该技术带来的弊端也十分显著。以下将作具体分析：

1. 使用个性化展示未向个人信息主体充分告知

法律法规或国家标准要求网络服务提供者在向个人信息主体提供个性化广告时，显著标明“定推”、“广告”，并要求网络服务提供者在隐私政策中充分披露对个人信息进行画像并会用于定向推送的场景和对用户可能产生的影响，就是为了实现对个人信息主体进行充分地告知的目的。但是实践中，未向用户告知或未向用户充分告知的违规情况其实有很多。

关于标注标识，网络服务提供者常常出现的问题可能有：（1）未标注“定推”、“广告”的个性化广告；（2）即使标注了“定推”、“广告”，这些字样却不够显著突出，例如字号很小，颜色不容易与页面其他内容进行区分，标注的内容位于页面角落不明显位置等，不能达到充分引起用户注意并进行谨慎判断的效果；（3）标识不足以明示相关内容是基于个性化展示生成，比如“为你推荐”、“推荐”等；或者 4）电商类平台的个性化广告难以划定清晰边界。

比如在南都的测评中，所有提供了关闭/推出个性化展示开关的19款App均将其设为默认开启，而只有五款App显著标明了个性化展示的内容，意味着剩余App的用户很可能看到个性化展示的内容而不自知；即使知道，也无法与非个性化展示的内容区分开，有损用户的知情权。

从实际操作情况看，对个性化广告进行标记的第一步是先甄别某个广告是否为“个性化广告”，但这一点在电商类平台较难判断及划清边界。

以淘宝为例，淘宝的营销平台“阿里妈妈”介绍了几类淘宝商家可以进行推广营销的方式：第一类是“淘宝直通车”，商家可以通过买搜索词的方式，让该商家的商品出现在显著位置。据测评发现，在某个搜索词下，一般第1个和第12个是广告位，出现在此位置的搜索结果会标有“广告”字样。但实测发现，不同用户搜索同样的词，第一个标有“广告”的搜索结果也不相同，所以可以推测这类广告很可能属于个性化广告，淘宝会根据用户的浏览历史、兴趣偏好等进行推荐。

图17：阿里妈妈平台上的“淘宝直通车”

第二类是“超级推荐”，商家可以在“猜你喜欢”、“有好货”、“今日头条”等栏目下打广告。实测发现，这类商品是根据用户的浏览历史、兴趣偏好等进行推荐的，符合《个人信息安全规范》个性化展示可以通过不同栏目分别展示的规定。

图18：阿里妈妈平台上的“超级推荐”

图19：淘宝“有好货”“猜你喜欢”等栏目进行个性化展示

此外，根据《电子商务法》第四十条规定，电子商务平台经营者应当根据商品或者服务的价格、销量、信用等以多种方式向消费者显示商品或者服务的搜索结果；对于竞价排名的商品或者服务，应当显著标明“广告”。

如，在一款App中，用户所看到的首页推荐信息中，通过竞价排名系统显示的内容也应被视为个性化广告，而且其中部分广告也使用了用户画像进行的展示。但在测评中，我们无法客观判断哪些是竞价排名哪些不是，因此在分数中未对此类个性化广告进行判别和打分。

关于隐私政策，网络服务提供者可能出现的问题有：(1) 未在隐私政策中对个性化展示的适用进行充分披露，或者没有将该机制作完整表述。从南都的测评分析中可见，不在隐私政策中向用户进行充分告知的问题在实践中依然存在。(2) 即使在隐私政策中披露个性化展示的相关内容，披露内容可能并不充分，或者由于相关条款表述不清晰简明、过于冗长或者披露内容不充分等原因，难以让缺乏互联网技术经验的用户对个性化展示的涵义、个性化展示对自身权利可能产生的影响产生有效的认识。(3) 对用户进行披露与告知的位置过于分散、隐蔽，一般用户客观上很难充分全部掌握披露的内容等。以上行为，在使用个性化展示的场景下，都很难能让用户对个性化展示有充分的认知，并作出符合其真实意思的判断，从而有违个人信息保护的透明性原则。

2. 使用个性化展示未征得个人信息主体的同意

如前所述，个人信息属于个人主体的基本权利，与个人信息主体的基本利益密切相关，因此任何对个人信息的处理，都应当征得个人信息主体的同意。

实践中，以App为例，可能存在以下方面的问题：

（1）由于隐私政策未详细披露使用个人信息进行个性化展示的场景以及对用户可能产生的影响等问题，对用户进行画像以及个性化展示，并没有征得个人信息主体的同意，违反了征得用户同意的个人信息保护原则。

（2）强制用户同意个性化展示功能，用户如不同意就不能使用产品功能，或者个性化展示与其他产品/服务的功能捆绑在一起，用户被要求一揽子同意等，违反了个人信息保护的最小必要以及选择同意原则。例如，网络服务提供者在隐私政策中要求用户同意使用个性化展示服务，如不同意隐私政策则直接退出服务，但是客观上，用户拒绝个性化展示服务有可能并不影响用户使用网络服务提供者提供的服务。又如，对于利用Cookie技术跟踪收集用户个人信息，并对用户进行画像的，虽然平台服务提供者有时可能会通过Cookie banner向用户提供选择同意使用Cookie记录其个人信息的选项，但是有时用户只是同意Cookie为提供产品服务便利性的目的采集其个人信息，并不同意网络服务提供者利用采集到的个人信息进行个性化展示，此时如果网络服务提供者只给用户提供一个统一的“同意”选项，即使用户点击了同意，其对于使用个性化展示的同意也是被动的，并非出于其真实的意愿。

（3）隐私政策中对于个性化展示的场景、个性化展示对用户可能产生的影响等问题表述不清，过于冗长晦涩，或则披露的位置过于分散、隐蔽，利用一般用户缺乏行业经验，不能充分知悉、理解和预估个性化展示意义的弱点，致使用户作出不能反映其真实意思的选择。此时，即使用户点击了“同意”，客观上也不应就此认定为该选择具有法律效力或视为对其自身权利的放弃。

3. 未赋予个人信息主体对个性化展示的自主控制机制

个人信息主体的自主控制权是实现对个人信息保护的重要方式。通常可能涉及以下几方面：（1）用户是否能够撤回同意，关闭个性化展示；（2）用户是否享有编辑个性化标签的选项，是否具有集中管理个性化标签的系统；（3）用户关闭个性化展示后，网络服务提供者能否删除或匿名化已经收集的用户个人信息等。

南都测评显示，虽然20款被测App均来自国内头部企业，但真正能让用户快速找到关闭/退出个性化展示按钮的是极少数，绝大部分App都要经过五次以上甚至上十次跳转才能找到。此外，还有一些App对关闭/退出个性化展示设置了有效期，在一定程度上削弱了用户的控制权。

在标签管理方面，除了“一键关闭”的形式，多数App采取的是在广告旁提供一个可以关闭单个广告的按钮。这一做法对用户来说只能关闭单个广告，需要多次操作。但对商家来说，则可以根据用户关闭广告的动作，调整用户的标签画像，更加精确地判断用户对广告内容的喜好。

实践中，我国存在网络服务提供者能够撤回同意，关闭个性化展示功能的情形，也存在部分产品未向用户提供个性化展示功能的例子。对于关闭个性化展示的方式，又可以分为一键关闭、逐项逐次关闭两类。显然，后者为用户实现自主控制权利所需付出的成本较高。有时，网络服务提供者甚至故意将关闭的渠道设置得较为隐蔽，用户可能需要经过多层点击才能最终跳转到关闭的页面，这对缺乏互联网技术经验的一般用户来说，具有实际操作上的困难。这几种方式究竟哪一种更好、更尊重用户的选择权，是否有利于平台描绘更精准的用户画像，是一个值得讨论的问题，这突显了隐私设计在保护用户权利与增强企业服务能力中的重要作用。

我国的部分网络服务提供者能够提供用户编辑画像标签的渠道，但是较少能提供集中的标签管理系统，供用户管理自己的个性化标签，这一点在本次南都的测评中就有体现。即使用户对标签内容能够进行编辑，目前也仅限于编辑网络服务提供者提供的公开的固定标签，而非通过用户画像形成的特定化的个人标签。

此外，用户还可能无法要求网络服务提供者删除个人信息。虽然在技术层面上，删除各种算法形成的用户画像数据存在一定难度，但是网络服务提供者是否对用户进行了相关承诺、是否在用户撤回接受个性化展示服务同意后采取了合理努力，对已经采集的个人信息进行删除或匿名化等措施等，仍是不同类型的网络服务提供者在个性化展示场景下对个人信息保护方面应该努力进行的尝试。

4. 使用个性化展示技术缺乏安全保障措施

如前文所及，个性化展示服务依赖于对用户进行精准的画像，因此必然需要收集越全面越好的用户个人信息。而随着网络技术的普及，网络服务提供者服务的对象范围也越来

越大，其处理的个人信息总量也相当庞大。为了保障所收集的个人信息安全，需要具备相匹配的安全保障措施，但是实践中很多网络服务提供者在积极努力地提升商业化变现的技术能力，却往往忽视加强自身安全能力建设。

例如，对于数据存储无充分的加密措施。有的网络服务提供者甚至明文存放用户个人信息，用户个人信息几乎处于“裸奔”的状态，保护程度非常低，一旦信息系统遭到攻击，发生数据泄露事件，那么就会存在用户个人信息随时被拖入暗网售卖的风险。2019年，德国巴登符登堡州数据保护局就此在德国境内开出第一例基于《通用数据保护条例》（General Data Protection Regulation，以下简称“GDPR”）的罚单，原因正是涉案聊天社交平台Knuddels.de公司以明文方式存放其用户的账号密码，黑客攻击了该平台后，导致约808,000封电子邮件地址和180多万个用户名和密码曝光，同时公司还在部分提供云存储服务的网上以明文形式公布了这些信息。2019年1月，上海市通管局对上海某传媒技术有限公司做出了行政处罚，认为其存在安全缺陷、漏洞等风险，并在接到通报和责令改正的要求后未采取补救措施。[8]

又如，网络服务提供者未设置企业内部员工的分级访问权及内部审批控制流程。即使在合法、合理地处理用户个人信息用于个性化展示场景下，网络服务提供者如果不对访问用户个人信息的内部员工设置访问权限，也将违反个人信息保护最小必要等原则。2018年，Uber公司因为未如它所承诺的那样密切监察其员工获取消费者和司机信息的权限而遭到FTC处罚，FTC认为其构成了对消费者的欺诈。而国内某快递公司员工利用自己是员工的便利条件，获取公民个人信息，并向其他内部员工购买后进行出售以获取非法利益的行为，被法院认定为构成侵犯公民个人信息罪。[9]

5. 个性化展示进行信息共享无授权

在某些情况下，网络服务提供者运用个性化展示功能时，可能会涉及个人信息在多个主体间流转的情况。比如，在投放个性化广告的案例中，个人信息采集的主体与个性化展示的主体有可能分离，法律关系链由“用户—个性化展示主体”，变为“用户—个人信息采集主体—个性化展示主体”。这种情况下，个人信息采集主体所收集到的用户个人信息可能会共享给个性化展示主体，即，出现【用户——个人信息采集主体】、【个人信息采集主体—个

[8]参见http://shca.miit.gov.cn/info/2622。最后访问时间2020年9月20日。

[9]参见https://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?docId=34bf1f8936fc4b3a8e9fa94c014cce06。最后访问时间2020年9月20日。

性化展示主体】、【个性化展示主体—用户】三对法律关系。

我们理解，通过三重授权，可以解决以上三对法律关系的正当性问题，但是需要特别注意的是，信息流转过程中，不同主体间的授权范围一旦超出用户同意范围之外，那么个人信息采集主体、个性化展示主体可能会面临未征得用户授权同意就处理其个人信息的合规风险，相应地，也就需要承担超出授权范围的相关责任。另外，个人信息采集主体与个性化展示主体间的链条不宜过长，如果间接采集个人信息并流转的线路太长了，就不好控制对个人信息来源的合法性、用户授权的实际范围以及层层的授权关系是否完整。

综上，无论是个人信息采集主体、个性化展示主体，还是用户本人，都需要通过订立合同的方式（无论是在线协议还是线下合作协议），明确各自的权利义务边界，以及可能的责任承担形式，以降低因授权瑕疵所带来的刑事与行政风险。

五、个性化展示合规管理的域外经验

（一）欧盟部分

1. GDPR以及各DPA的指引

欧盟背景下没有专门针对个性化展示的指令或者条例，而是通过概括的GDPR以及针对特定场景（如直接营销）的指南进行规制。

根据GDPR第22条，ARTICLE 29 DATA PROTECTION WORKING PARTY（以下简称“WP29”）以及英国数据保护机构（Information Commissioner’s Office，以下简称“ICO”）[10]的指引[11]，GDPR对个性化展示的规制主要涉及两个制度，即基于用户画像（profiling）的决策和基于自动化的决策（automated decision-making）。

关于用户画像。ICO在其《精准化营销法》（“Direct Marketing Code”）中提出，用户画像是指将个人的行为特点进行分析，以用来得出用户的偏好、预测用户的行为、作出与用户相关的决策、或者将用户分类到不同的群里或领域的行为。ICO明确要求，进行任何用户画像行为、或者从第三方（如数据经纪人，data brokers）购买用户画像信息的行为必须符合GDPR的要求以及适用《2003年隐私和电子通信（EC指令）条例》（以下简称PECR）[12]的规定。

关于用作追踪与画像的Cookie技术。通过Cookie及同类技术在线追踪、记录用户个人信息已经成为实现对用户进行画像、对用户进行个性化展示的重要手段。因此，GDPR将记录用户信息的Cookie作为个人信息的一类进行保护，对于使用Cookie技术的态度是：网络服务提供者必须告知用户收集和处理Cookie的目的；用户必须在Cookie数据收集开始之前给予特定的、自愿的、明确的和针对该处理行为的同意；用户继续浏览网站的行为并不表示该用户同意；同意条款和条件（terms and conditions）不视为获取同意处理Cookie的方法；用户必须能够识别所有处理其数据的关联方等。

基于用户画像作出的一般决策。根据GDPR第21条，数据控制者在具有高于个人信息主体权利和自由的合法事由，或为主张法律诉求所需要时，可以使用用户画像或使用画像作出

[10]虽然英国于2020年1月31日脱离欧盟，但考虑到英国现在进入脱欧过渡期，实际上依然需要执行欧盟的各种规则，并且英国计划在脱欧过渡期后将GDPR纳入其法律体系中，所以本报告仍将英国部分纳入“欧盟部分”一同进行讨论。

[11]参见ARTICLE 29 DATA PROTECTION WORKING PARTY: Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Adopted on 3 October 2017。

[12]参见Privacy and Electronic Communications (EC Directive) Regulations 2003。

的决策，否则数据主体有权拒绝使用用户画像或使用画像作出的决策；如果数据控制者使用用户画像的目的在于向用户进行直接营销（direct marketing），用户享有直接拒绝此类画像的权利。

对基于用户画像作出的一般决策，数据控制者应当遵循GDPR关于个人信息保护的一般性规定。比如，数据保护基本原则、数据处理的合法依据[13]（例如，事先应取得个人信息主体的同意等）、处理特殊种类个人数据的要求以及满足数据主体的相关权利（例如，保障用户的知情权、删除权、修改权等）等。ICO发布的《直接营销准则》进一步要求，如果组织进行“大规模用户画像”或者“财富画像”，则需要在开始处理前完成数据隐私影响评估（DPIA）。当利用用户画像时，组织需要确保符合GDPR和PECR的规定。仅仅只是接受第三方对于他们提供的数据是符合规范的保证是不够的，组织必须能够证明其合规性且对处

作为规划阶段的一部分，组织需要在开始使用用户画像前完成适当的尽职调查。尽职调查可以包括回答以下问题：

（1）第三方履行透明度要求的方式—公众是否知道该公司拥有他们的数据？

（2）第三方使用数据的来源—来源是否合理？

（3）第三方进行DPIA的结果—是否有完成该评估？

（4）数据是何时汇编的—数据已被持有多久？

（5）同意的记录（如果是通过同意收集的数据）--数据主体同意的内容、同意时他们被告知的内容以及授予同意的方式。

（6）是否存在任何特殊类型数据？

基于用户画像作出的自动化决策。虽然自动化决策在形成过程中没有进行任何人为干预，但其形成的结果却很可能对数据主体产生严重影响（比如影响到数据主体的选举权等重大权利等），因此，区别于一般用户画像和基于用户画像决策，GDPR对基于用户画像作出自动化决策的适用设定了更为严格的要求：GDPR第22条采取原则上禁止适用，但设定某些例外情况的模式。例如经过数据主体的明确同意，或为订立或履行数据主体与数据控制者间合同所必需等。GDPR还要求在此情形下，控制者应保证数据主体的知情权和访问权等。采取此种更加谨慎的态度，是为了避免这种没有人为纠偏机制下产生的不正义和歧视问题。

[13]根据ICO《直接营销准则》的说明，正当利益（legitimate interests）这一依据是不大可能适用于为了直接营销的目的而进行打扰性用户画像（intrusive profiling）的。这种用户画像一般并不在个人合理期待范围内而且也很少足够透明。具体参见《Direct Marketing Code》（Draft）第58页，https://ico.org.uk/media/2616882/direct-marketing-code-draft-guidance.pdf。

当然，基于用户画像作出的自动化决策与作出一般决策相同，组织同样需要遵循GDPR关于个人信息保护的一般性规定，例如，上文提及的数据保护基本原则、数据处理的合法性基础（例如，事先应取得个人信息主体的同意等）、处理特殊种类个人数据的要求以及满足数据主体的相关权利（例如，保障用户的知情权、删除权、修改权等）等。

2. E- Privacy Regulation的相关规定

欧洲理事会通过的e-Privacy Regulation（以下简称“ePR”）与GDPR同属为落实《欧盟基本权利宪章》而进行的立法，与GDPR之间相互补充[14]，均为欧盟数据保护框架的重要组成部分，其对于通过个性化展示方式处理用户个人信息的行为也有相应的规则。

ePR认为从个性化展示研究的范围来看，用户通过在线行为交互的内容能够对用户进行画像。根据第6条规定，通过在线追踪技术处理此类信息应当取得用户的同意，或者处理用户此类信息是为了向终端用户提供特定服务所必须。在征得用户同意后，还应当给予用户随时撤回同意的权利，并就该撤回同意的权利每隔6个月向用户进行提示。

ePR第10条规定，软件服务提供者应当向用户提供隐私权设置（Privacy Settings）的机制，并提醒用户主动进行设置或同意某种隐私设置。软件服务提供者还应当向用户提供拒绝第三方主体在终端设备收集或存储用户个人信息的选项。这要求技术提供方在对用户使用的终端设备进行默认设置时，默认关闭允许第三方存储或使用用户终端设备中产生的任何信息，只有在用户明确同意允许第三方在设备中设置Cookie等同类装置时，第三方才可以对用户的信息进行收集或存储。

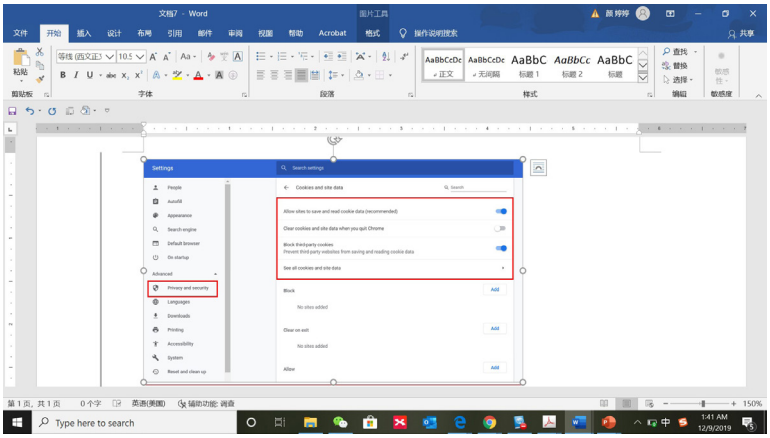


图20：谷歌浏览器提供隐私设置版面，供用户进行隐私设置管理

[14]参见Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)，https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf，最后访问于2020年9月18日。

此外，ePR第8条原则上禁止使用终端设备处理或存储用户个人信息，除非有正当的事由。ePR第7条规定，用户的在线数据在被接收方接受后，网络服务提供者应当及时删除用户的在线数据或者对其进行匿名化处理等。

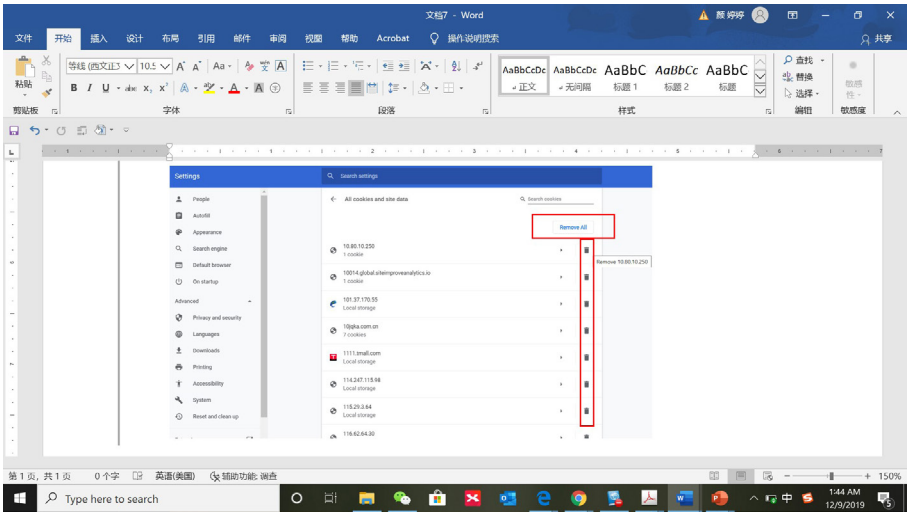


图21：谷歌浏览器提供集中的用户选择删除Cookie、Cookie记录信息的选项

3. 对儿童进行画像与个性化广告的规定

GDPR不鼓励对儿童进行画像和自动化决策等类似效果的动作[15]，为营销或者画像目的处理儿童个人信息的，需要对儿童个人信息进行特殊保护[16]，如通过DPIA来证明该数据处理活动对儿童的权利和自由没有影响。此外，根据英国CAP规范[17]，通过使用个人数据进行定向广告投放时，广告主必须表明他们已采取合理的措施，以减少对处于或可能处于受保护年龄段的人接触该年龄所限制营销的内容。《2018年视听媒体服务指令（AVMSD）》要求，出于保护儿童目的，不应将从内容中收集或生成的个人数据用于商业目的，而使未成年人可能遭到身心或道德上的损害，例如使用直接营销、画像和针对未成年人行为的广告。此要求与GDPR的目的限制原则以及与ICO发布的2020生效版《适龄设计：在线服务实践规范》中的指南相符。

[15]GDPR recital 第71条。

[16]GDPR Recital 第38条。

[17]全称The UK Code of Non-broadcast Advertising and Direct& Promotional Marketing. 参见www.asa.org.uk/codes-and-rulings/advertising-codes/non-broadcast-code.html。最后访问时间2020年9月20日。

4. 执法案例

Google定向广告推送未保障用户知情同意权受CNIL调查

2018年5月，法国国家信息与自由委员会（以下简称“CNIL”）调查发现，Google定向投放广告涉及GDPR规定的数据处理原则以及处理的合法性问题、从数据主体处/非从数据主体处获取信息的问题，以及数据主体的“同意”问题等，具体涉及以下方面：

1、违反透明性原则。一方面，用户无法了解Google“大规模、侵入性的”数据处理达到了什么样的程度；另一方面，Google未提供用户数据的便捷访问渠道（例如数据处理目的、数据存储时间或用于个性化广告的个人数据类别，过度分散于多个文件中），需要经过五六个步骤才能访问到，使得用户无法管理其个人信息。

2、违反GDPR同意要求。Google将用户“同意”选项设定为“全局默认设置”，不符合监管机构所规定的“特定同意”要求。Google要求用户须整体同意隐私政策中的服务条款和数据处理条款，而非区分各种不同目的（如个性化广告或语音识别等）来同意各项条款。

3、Google用于征求安卓软件用户个人信息的弹出式窗口暗含威胁意味：“如果用户不接受这些条款，服务将无法提供。”并预先勾选了个性化广告的显示框，而根据GDPR的规定，只有用户明确的肯定行动（例如勾选未预先勾选的显示框），同意才是明确、有效的。

因Google在处理个人用户数据时存在缺乏透明度、用户获知信息不便、推送广告缺乏有效的自愿同意原则等问题，CNIL对其处以5000万欧元，约合3亿8千万人民币的罚款。

英国法院判定Google擅自植入Cookie收集用户浏览器信息违法[18]

2015年，三名英国公民起诉Google公司，主张Google通过在苹果Safari浏览器中植入DoubleClick ID Cookie的方式，在未向用户告知、未征得用户同意的情况下，采集用户使用Safari浏览器时产生的数据（Browser Generated Information），例如，上网记录、上网习惯、社会地位、种族与民族、性取向、经济状况、精神与身体健康情况等个人信息。Google采集用户的个人信息后，对用户进行个体画像，并通过向用户推送个性化广告的方式进行盈利。尽管Safari网页浏览器默认的隐私设置允许用户从第三方跟踪用户的Cookies中退出，但尽管如此，用户的个人信息仍会通过“Safariworkaround”被收集，在相关时期，由于Safariwork-around的运行，并且在用户尚未知晓或同意的情况下，Google会由此获得并记录了上述有关的私人与个人信息。Google在上诉法院的判决中败诉，后寻求向英国最高法院进行上诉。

类似的情况还有：2018年，英国苹果手机用户组成Google You Owe Us的组织，意图向Google发起集体诉讼，要求Google就其避开苹果公司防止第三方跟踪用户Cookie机制、在不征得用户同意的情形下收集个人信息用于个性化展示的行为进行巨额赔偿。

[18]参见https://www.supremecourt.uk/news/permission-to-appeal-decisions-28-july-2015.html，最后访问于2020年9月18日。

（二）美国部分

1.FTC规则

对于个性化展示行为的合规性要求，美国在联邦层面没有专门的成文法规定。但作为消费者权益保护的主要监管机构--美国联邦贸易委员会（Federal Trade Commission，以下简称“FTC”）从1999年开始一直关注并持续研究该课题（个性化广告），并通过多次与消费者、企业、行业自治组织等多方商谈，提出了解决该问题所引发隐私保护风险的建议性规则。

FTC指出，用户对个性化广告行为的知晓程度、企业向用户披露处理其个人信息的必要性、企业对所收集信息的使用和保护、以及保护数据的标准等问题是个性化广告行为中隐私保护问题的关键。经过多轮讨论，在充分尊重用户自治、强调行业自治的基础上，FTC提出以下建议性规则：

（1）透明度与消费者控制原则

网络服务提供者应当提供清晰、简洁、突出的、用户友好型陈述，告知用户在线被收集个人信息用于画像并进行后续推送的目的。用户享有接受或拒绝对其进行定向推送的行为，网络服务提供者应提供清晰、容易使用与获得的方式供用户实现上述拒绝权。例如：Facebook能在“广告偏好”设置中，根据“你的兴趣”、“广告商和企业”、“你的资料”等类别，选择关闭或开启与其相关的个性化广告推送。用户还能在设置页面中，了解到广告主的目标受众与被投放广告的用户间有怎样的联系。

图22：Facebook广告管理页面

Twitter在注册时，会弹出是否接受个性化广告的开关按钮，用户可设置、编辑、删除系统的标签。而在“兴趣与广告数据”设置中，用户也能查看并自主添加Twitter平时根据用户的行为标记出来的用户兴趣爱好等特征值。

图23：Twitter个性化广告的开关按钮以及编辑、删除标签选项

Google也提供在其“个性化广告”设置中直接查看Google基于用户的网络浏览历史等信息为用户打的标签，而且用户可以直接删除自己不想要的标签。

图24：Google个性化广告的开关按钮以及编辑、删除标签选项

值得注意的是，与20款被测App中五款提供标签编辑功能的App不同，谷歌展示的标签基于用户个人的使用偏好和画像，更加细致也更具多样性，比如“25-34岁”、“爱情电影”、“产品测评和价格比较”等，而非系统统一设定的固定标签。这大大增强了透明性，增加了用户自主调控个性化展示相关程度的能力。

图25：谷歌实现“一键关闭”个性化广告的面板

(2)数据安全与限期保留原则

网络服务提供者应当提供合理的数据保护措施，具体措施应综合考虑数据的敏感性、信息网络服务提供者的商业实践、个性化广告行为面临的风险类型以及实际可采取的合理措施等因素。同时，网络服务提供者应仅在必要的时间范围内，为合法的目的处理个人信息。

(3)隐私承诺变化的同意原则

网络服务提供者应当按照其承诺的方式处理个人信息。否则，如果实际处理方式与承诺有实质性变更，其应征得个人信息主体的明示同意。

(4)个人敏感信息明示同意原则

网络服务提供者处理个人敏感信息应当取得信息主体的明示同意。FTC对于是否应直接禁止网络服务提供者处理个人敏感信息有待进一步讨论。

以上原则提出后，很多企业纷纷修正自己的行为，取得了良好的效果。2011年，FTC收集公众意见后对以上原则进行修订，总体上保留了四项原则，同时对原则的具体内涵作出更为细致的提示。例如，对于透明度与消费者控制原则，FTC补充强调，针对不同于传统网页端的移动设备或互联网服务，应当相应地建立适用各自场景的有效的用户告知的机制。对于隐私承诺变化的情形，应当适用更为灵活的机制，如显著地告知消费者、赋予消费者以选择退出机制来应对等。

尽管FTC提出的以上规则性质上属于建议性规则，不具有法律强制力，但是，FTC享有来自于《联邦贸易委员会法》第5条等法规的授权，相关法规禁止网络服务提供者在市场中实施不公平或欺骗性的行为。根据此条款，FTC有权对未遵守公布的隐私政策和未经授权泄露个人数据的公司采取强有力的执法行动。

2.DAA行业自律规范

美国数字广告联盟（Digital Advertising Alliance，以下简称“DAA”）在其2009年7月发布的《在线行为广告自律原则》(Self-Regulatory Principles for Online Behavioral Advertising)中，采纳了FTC对于在线行为广告（Behavioral advertising）的定义，并确立了在线行为广告领域个人信息保护七大基本原则，包括：

(1)教育原则（Education）：第三方、网站以及服务提供商应当向消费者及相关企业介绍在线行为广告相关知识、《在线行为广告自律准则》的内容以及消费者选择机制；

(2)透明性原则（Transparency）：第三方、网站以及服务提供商在收集使用消费者个人信息时应履行提示告知义务；

(3)消费者控制原则(Consumer Control):赋予消费者选择是否允许以在线行为广告为目的对其网上活动信息的收集和利用;

(4)数据安全原则(Data Security):第三方、网站以及服务提供商应当采取合理措施保障消费者个人信息的安全,对个人信息的保留限于在线行为广告必要范围内;

(5)实质变更原则(Material Changes):第三方、网站以及服务提供商对数据收集和使用政策进行实质性或者重大变更前应当取得消费者明示肯定的同意;

(6)敏感数据原则(Sensitive Data):对敏感数据的收集和使用要特殊对待;和

(7)问责原则(Accountability):为保障消费者个人隐私权益,自律组织的成员单位合力构建在线行为广告良好生态系统,美国商业促进局和直销协会合作共建与《在线行为广告自律原则》配套的问责与执行机制。

迄今为止,DAA已经是整个数据生态的领导者,可以要求网站、应用的发布者以及品牌广告商等承担相应的义务。例如,由互联网领先的广告商,包括24/7 Media, AdForce, Ad-Knowledge, Avenue A, Burst! Media, DoubleClick, Engage, and MatchLogic等组成的网络广告联盟(Network Advertising Initiative,以下简称"NAI")已于2010年加入DAA。由此可见,DAA的行业自治规范在美国具有广泛的影响力。

3. 对儿童进行画像与个性化广告的规定

根据COPPA,依赖用户行为投放广告(behavior advertising)的行为不属于企业内部运营这一例外情形,因此收集使用儿童个人信息用于个性化广告的,需要满足COPPA的要求,即通知儿童的父母并获得其验证同意。

FTC Staff 在《在线行为广告自我监管报告》中指出,企业在使用儿童相关数据进行个性化广告(behavioral advertising)之前应当获取主动的明示同意。

另外,NAI规范要求运营者在进行个性化广告时满足(1)使用设备识别信息(DII)进行个性化广告时,需要建立opt-out机制;(2)使用敏感信息(包括儿童信息)进行个性化广告时,需要建立opt-in机制;(3)需要获得可验证的家长同意,并且NAI成员单位必须遵守COPPA规则。

《数字世界中加利福尼亚未成年人的隐私权法案》第25580要求运营者明确得知用户为未成年人时,不可对用户进行基于用户画像、活动记录或与未成年人联系地址信息的广告推送(不包括IP地址与设备识别码);并且还要求若运营者知悉用户为未成年人,且知悉第三方有意进行酒精饮品、枪支、弹药、烟草等的广告/市场营销,则运营者不可向第三方提供相关信息。

4. 执法案例

InMobi Pte Ltd.未经用户同意秘密追踪用户地理位置[19]

移动广告公司InMobi Pte Ltd.是一家通过SDK专门向移动设备投放广告的公司。因InMobi Pte Ltd.的客户想要实现将广告定向投放给某些国家消费者观看的功能，InMobi Pte Ltd.依靠IP地址，要求消费者许可其通过手机的内置收集用户Wi-Fi网络数据，提取信号强度、ESSID（网络名称）和BSSID（唯一标识符），通过这些信息，对全国各地的Wi-Fi网络建立了数据库，跟踪用户信息，并最终创建了一个可以间接追踪用户位置的系统。

2016年，FTC指控InMobi Pte Ltd.通过附近Wi-Fi路由器的标识符非法秘密追踪用户，即使用户不同意通过其手机的地理位置功能来被直接追踪，InMobi Pte Ltd.也会继续追踪他们，违反了FTC Act第5条。同时，由于InMobi SDK嵌入针对儿童的移动应用程序中，收集儿童信息时并未向家长进行通知，或取得家长的明示同意，该公司还被指控违反了COPPA（16 C.F.R. Part 312）。

InMobi Pte Ltd.最终接受了FTC的和解方案，同意为此支付95万美元的高额罚款；InMobi Pte Ltd.还必须删除其拥有地理位置信息的数据库以及收集的所有儿童信息；除非用户明确同意不得收集用户的位置信息，并尊重用户不被跟踪的选择；此外，InMobi Pte Ltd.还将建立用户隐私计划，接受未来20年每隔两年FTC的独立审计。

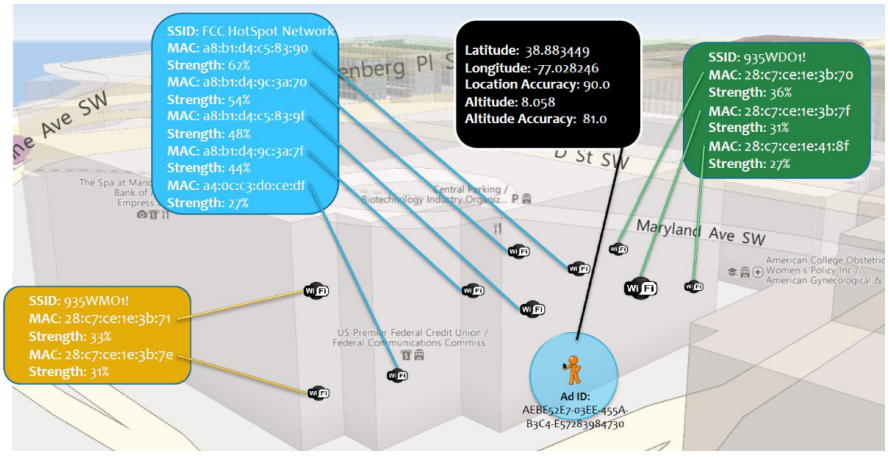


图26：InMobi通过WiFi收集用户信息示意图

[19]参见https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked，最后访问于2020年9月18日。

YouTube Kids未经儿童监护人明确同意利用Cookies收集儿童信息[20]

2019年，美国FTC和纽约总检察长指控Google旗下的YouTube在其视频分享服务中，使用跟踪儿童用户的永久性标识符（即Cookies）收集儿童个人信息，并向儿童投放定向的广告，且没有预先通知父母或征得父母的同意，违反了FTC第5条和COPPA规则（16 C.F.R. Part 312）。根据指控，YouTube已经通过向儿童定向推送广告赚取了数百万美元。

COPPA规则要求针对儿童受众的网站和在线服务在收集13周岁以下儿童的个人信息前，应当告知其信息被收集和使用的情况并获得儿童父母的同意，包括为了向用户推送个性化广告而使用永久性标识符技术来追踪其用户的互联网浏览习惯。此外，广告提供方等第三方，在有意识地直接从以儿童为受众的网站和在线服务中收集个人信息时，也应受到COPPA的约束。FTC认为，虽然YouTube声称其网站针对一般受众和用户，但YouTube的一些个人频道（例如由玩具公司经营的频道），都是针对儿童用户的，因此必须遵守COPPA规则。

该案Google、YouTube与FTC、纽约州政府最终达成和解，但其需要向FTC支付1.36亿美元、并向纽约州支付3400万美元的罚款。除了罚款之外，和解还规定：禁止Google和YouTube从已经收集的信息中获利；要求Google和YouTube遵守COPPA规则，在收集儿童信息时通知儿童父母、并获得父母同意；开发、实施和维护一套系统，该系统内允许频道所有者识别他们在YouTube平台上投放的专门针对儿童的内容，以确保它符合COPPA规定；此外，YouTube必须通知频道所有者他们所投放的专门针对儿童的内容受COPPA规则的约束，并为服务于YouTube频道的所有员工提供年度培训。

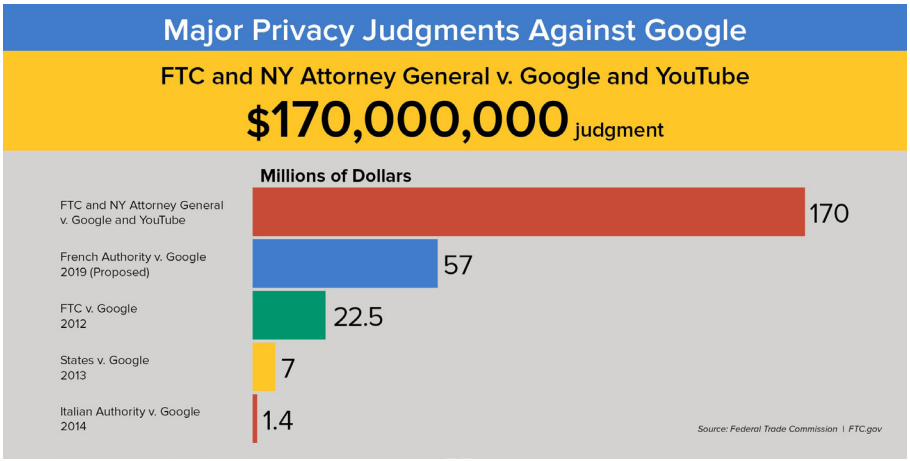


图27：FTC及其他国家执法机构对Google的处罚/和解金额

[20]参见https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations,最后访问于2020年9月18日。

Facebook未经用户授权向第三方共享用户的个人信息[21]

2018年3月，英美媒体曝光，英国政治咨询公司“剑桥分析”（Cambridge Analytica）在未获得用户授权的情况下，通过在线性格测试的方式获取了8700万Facebook用户的个人信息，并利用这些数据对美国选民定向推送政治信息。

FTC对Facebook的调查可以追溯回2010年，发现其未经授权将用户信息泄露给第三方，并使用带有欺诈性的描述和设置。2012年FTC和Facebook达成第一次和解，禁止Facebook虚假描述消费者自己可控的信息范围及Facebook允许第三方访问信息等内容，并要求Facebook将信息分享给第三方之前，必须提前向用户告知并取得用户的明示同意。而本次调查中，FTC发现Facebook的隐私设置和描述带有欺诈性，用户不知道自己有退出向第三方开发者分享数据的（opt-out）选项，也很难发现该选项，导致用户信息仍然被第三方开发者获取和使用。此外，在Facebook新开发的人脸识别技术的使用上，也存在类似问题。

FTC指控Facebook违反了FTC Act第5条，双方签署了2019和解令，要求其支付50亿美元赔偿金。同时，和解令还要求Facebook停止对用户的虚假描述内容，建设“全面隐私计划”保护数据的隐私性、保密性和完整性，并增加相关评估、审查和报告的要求。

[21]参见https://www.ftc.gov/enforcement/cases-proceedings/182-3107/cambridge-analytica-llc-matter，最后访问于2020年9月20日。

六、针对我国关于个性化展示的合规建议

本报告通过分析网络服务提供者提供个性化展示服务可能存在的法律合规问题，结合国外管理经验和实践做法，提出如下建议：

（一）尽快完善法律法规或国家标准，统一个性化展示行为的概念

针对目前我国立法呈现出分散式的特点，没有专门针对个人信息保护的统一立法，也没有关于个性化展示的单独立法。建议在层级较高的法律法规中补充与个性化展示相关的规定，比如在制定中的《个人信息保护法》中对通过画像与个性化展示中所涉及的个人信息保护进行规定，并且对《数据安全管理办法（征求意见稿）》等规范中对个性化展示条款进行进一步修订，厘清选择进入、选择退出以及标注“定推”在不同个性化展示场景中的适配性，统一不同层级法律法规或国家标准中个性化展示、个性化推送、定向推送、定推等概念，避免不同概念混乱使用的局面。否则，概念上的分歧可能会引发公众对行为性质不同的解读，影响法律规范的运用与执行。

如前所述，无论是2020年7月份工信部的整治要求，还是2020年9月20日国家网络安全周“个人信息保护主题日”上对画像与定向追踪机制的热议，国家监管层面以及标准层面均对个性化展示的安全与合规问题开始关注。收集、使用个人信息符合合法、正当、必要、明确、透明的原则，要让用户感知并有权决定其个人信息被用于画像和进行个性化展示/推送等，建立健康有序合法的互联网生态环境，建议尽快完善与个性化展示相关的行业标准、安全标准及指南，以给予各大互联网平台（包括App开发者）、广告主、广告服务提供商以及其他相关方有可落地的指导与建议。

（二）信息收集应当符合透明性原则，保障用户的知情同意权

个性化展示信息的处理应当符合用户的合理预期，个性化展示服务提供者应就个性化展示收集用户个人信息、可能产生的后果等事项向用户进行及时告知，并充分征得用户的同意。[22]这是因为，个性化展示服务收集用户个人信息非常广泛，这些信息的收集、聚合与利用很可能会给用户带来相应的风险。因此，在这种前提下，保障用户的知情权、选择权等权利具有很大的必要性。信息收集阶段的提示可以为消费者提供一定程度的警示与选择自由，也可以减少侵犯消费者权益的可能，帮助企业赢得用户更多的信任和好感。[23]此外，如前文所及，实践中网络服务提供者未对用户进行充分告知、或利用用户在网络

[22]丁晓东，用户画像、个性化展示与个人信息保护[J]，环球法律评论，2019(5)：82–96。

[23]朱芸阳，定向广告中个人信息的法律保护研究——兼评“Cookie 隐私第一案”两审判决[J]，社会科学，2016(1)：105–109。

技术领域经验的缺乏，设置各式障碍阻碍用户充分理解个性化展示服务的情况时有发生。因此，建议网络服务提供者把握风险点，真正做到以简单、易懂、直接的方式向用户进行披露并征求其同意，才能真正做到透明性原则的合规要求。

另外，企业还可以细化合规要求，通过隐私政策全面透明地告知用户将被收集哪类个人信息，用于画像和何种情形下的个性化展示或推送，将从哪些第三方处间接采集个人信息以及具体个人信息类型，可能将用户个人信息共享给哪些合作方协助开展个性化展示的事宜以及具体个人信息的类型。涉及处理儿童个人信息进行画像或者个性化展示的，不但需要透明告知（包括收集、使用、存储、与第三方共享数据等目的与具体的处理方法），还需要企业提前开展个人信息影响评估，告知家长或者监护人评估结论是否会影响到儿童的权利与自由。总体上应当坚持原则上禁止，除非经过家长或者监护人的明示同意。涉及处理个人敏感信息（如人脸信息、声纹信息）等进行的画像或者个性化展示，企业除了需要做到前述要求的告知同意，还需要考虑必要性与最小够用，应当对这些信息单独加密存储，建议最好在收集时不留原数据，只进行特征值或摘要信息的提取后处理。

（三）保障用户的自主控制权。

个人信息主体对个人信息享有基本权利与自由，保障用户的自主控制权，例如知情权、同意与撤回同意的权利、修改权、删除权等，能够为用户自主实现权利与自由提供创造途径，这是尊重用户基本权利与自由的基本保障。同时，用户的自主控制与参与，能够不断进行修正、删除和增加用户标签等管理行为，这些行为的交互能够反映用户的真实需求，使个性化展示的精准度进一步提升，从而能够为用户和网络服务提供者带来利益的共赢。具体而言，网络服务提供者应当为用户提供关闭个性化展示的渠道，且关闭方式应当简单、容易操作；网络服务提供者最好应向用户提供前台集中控制用户画像标签的系统，让用户自主进行删除、增加等，通过将后台标签前台化的思路，更好地展示企业的透明度，同时也赋予用户对运用其哪些个人标签进行个性化展示拥有更完整的控制权，另一方面也避免了当用户行使“用脚投票”对个性化展示一键关闭时企业的尴尬。如果有可能，企业可以考虑产品PbD的设计，既让用户享有一键关闭画像标签、不同类型个性化展示内容的权利，同时也可以在一键关闭机制下设置分层关闭的按纽，给予用户多维度且充分的选择权。

有观点认为，用户如果关闭个性化展示服务，网络服务提供者应及时删除（甚至是销毁）或匿名化处理此前基于该服务收集的标签以及个人信息，即使用户再次开启个性化展示服

务，也不能继续使用此前所收集的信息。但是，一旦用户再次打开个性化展示功能时，网络服务提供者只能从零开始重新建立用户画像，用户体验可能因此受到很大影响。因此，企业在提供关闭个性化展示服务时宜给予数据删除后果的充分告知，如有可能，也可以设计成两层按钮，第一层是关闭个性化服务但保存用户标签数据，以便用户再次打开此功能时不影响使用体验；第二层为关闭个性化服务且删除用户标签数据，并且告知用户可能产生的影响与后果。这样，既充分告知并尊重了用户的选择，也为企业不被投诉产品体验差、不智能而提供较为稳妥的解决方案。

目前《个人信息安全规范》中对画像和自动化决策的限制有相关规定，如对用户画像中个人信息主体的特征描述和在业务运营或对外业务合作中使用用户画像的限制，另外也规定了，使用个人信息时应消除明确身份指向性，避免精确定位到特定个人，除非获取个人信息主体的授权。同时，还可以考虑参考GDPR对通过用户画像进行一般性决策与自动化决策的不同保护要求，企业如果实施后者的，可以给予一些加强性保护措施，比如保证数据主体的知情权、访问权、撤回同意权等个人信息主体的基本权利。如果发现自动化决策可能会对个人信息主体产生重大影响的，企业可以在适当时候采取人工干预机制，以确保当决策出现偏差时能够及时被纠正。如果涉及到个性化广告跨平台推送的，企业不仅应当在隐私政策中说明，也需要给予退出和关闭机制并且需要匿名化处理退出后的标签。

（四）保障用户被处理个人信息的安全。

如前文所及，随着个性化展示收集的个人信息精准度的进一步提高，网络服务提供者收集个人信息的也必将越来越广泛。随着网络技术的不断普及，使用个性化展示服务的用户增多，网络服务提供者往往掌握的用户画像的数据量也将是海量的。尤其对于与个人权益密切相关的行业，如金融行业等，往往涉及重大敏感信息的收集，一旦发生泄露等其他信息安全事件，给用户、社会甚至国家造成的损失将难以估量。因此，这要求网络服务提供者建立起与其所处理的个人信息敏感度、重要性、数据量等相匹配的安全保障能力，最大程度上避免灾难的发生。

提供个性化展示服务的网络服务提供者需采取相应的技术措施以保障个人信息的安全，防止个人信息泄露或滥用风险。例如，在数据采集阶段，可以采用数据隔离、加密等方式保障缓存在本地终端的数据安全；在数据传输、存储阶段，采用数据隔离、加密、去标识化等方式降低因数据泄露造成的用户损失，尽量按照最小化原则保存个人信息；在数据使

用画像制作阶段，尽量消除个人信息的身份指向性，加强展示时的脱敏处理以及个人信息访问控制管理；在数据销毁阶段，及时响应个人用户要求以及App开发者代表个人用户发出的数据删除的请求。在画像与标签数据的保存要求上，也需要符合最少必要，有限存储的原则。此外，个性化展示服务的网络服务提供者，应采取必要措施保障基础设施、业务系统等方面的网络安全，完善安全应急响应机制和应急预案，防范因黑客攻击造成数据泄露等安全风险，同时强化自身安全事件应急处置能力。特别地，当iOS系统对收集IDFA要求用户明示同意和Android系统不再适用收集IMEI信息时，企业如需开展个性化广告业务，鼓励创研自有不唯一的可变更的设备ID以更好地保护用户的隐私。

（五）个人信息共享需征得用户同意。

总体上网络服务提供者利用其合法收集到的信息与数据进行用户画像、帮助生产经营将是未来社会发展的方向。毕竟，信息的定向推送、数据的融合与利用是互联网与大数据的本质所在。在用户允许/授权的范围内，开放用户信息与第三方进行共享，可能会给商家和用户带来双赢。但是，数据共享仍可能涉及不同领域的法律风险（如个人信息保护、不正当竞争等），因此，进行数据共享的网络服务提供者应当承担数据的安全保障义务。

首先，应当征得个人信息主体的同意，取得个人信息主体对网络服务提供者向第三方共享、或接受第三方共享其个人信息的授权，保障各授权链条的合法性。其次，网络服务提供者还应在第三方进行数据共享前与数据接收方订立协议，明确双方的权利与义务，并要求数据接收方以相同或更高的标准保护个人主体的个人信息安全等。此外，如有需要，可以在共享前进行相应的风险评估，以最大化地降低风险。

另外，在保护个人信息的同时，也要兼顾产业的良性发展，把握好隐私保护与经济可持续性的平衡。比如说针对个性化广告投放，在用户同意了平台隐私政策后，企业可以对个性化广告进行标识（如设置个性化展示的分区，或者认为同时标注定推与广告太不美观的话，可以创设一个代表“定推”的行业性Logo标注）并给予退出或关闭个性化广告的路径（如致电客服退出或者在隐私界面上设置关闭按钮）。在满足上述合规前提下，隐私界面的个性化广告按钮可以设定为不默认关闭（除非是提供儿童专项产品的平台或者是平台提供的儿童保护子平台需要默认关闭个性化广告展示），当用户不希望收到个性化广告时可以通过将按钮滑向Off实现退出。本报告第二章第一节所提及的《互联网个人信息安全保护指南》的相关条款应该也有此考虑。通过显著地告知消费者、赋予消费者以选择退出机制（变化且动态的同意与撤回同意方式）既可以保护广告业的发展，同时也能够实现用户的个人信息保护的权利。

（六）鼓励企业开展行业自律。

个性化展示依托的互联网技术发展日新月异，催使个性化展示业务形式的更迭速度也十分迅速。鉴于企业是位于生产发展第一线的主体，其对于制度背景的了解程度、制度建设的需求程度也最为敏锐。建议国家鼓励提供个性化展示的企业开展行业自律，发展行业自治规范，作为立法、监管等国家公权力的补充力量。

在面对我国当下法律法规或国家标准不完善、或者随着技术发展出现的新问题时，企业往往能充分发挥发挥其专业性、灵活性、及时性、经济性等优势，协助国家机关共建个性化展示服务发展的良好生态。同时，行业自律组织的问责往往对于企业来说具有良好的震慑效果，企业为了业内声誉等因素的考量，往往也会更加自觉地遵守行业自律规范。

（七）建立有效的问责机制。

我国目前还没有类似美国FTC的专门的强势执法机构，这导致我国的法律法规或国家标准在实践中被遵守的程度并不高。当然，随着四部委2019年专项整治App等系列行动的开展，我国执法机构的强力执法效果也已经开始显现。但是，为了更加迅速、有效地保障消费者个人隐私权益，我们可能仍然需要在有执法权的国家机关之间的明确职责分工，同时也要在不同层级国家机关之间明确职责分工，以避免多头执法、多头观点不一、重复执法、层级分工不均等因素导致整体执法效率低下、执法局面混乱的风险。此外，建议政府执法机构与行业自律组织的成员单位合力构建个性化展示的良好生态系统，共建与行业自治规范相配套的问责与执行机制，以最大程度地实现用户的权益。对于合规工作进行地比较好的企业，可以发布年度问责报告（如企业合规白皮书等）向用户公示企业在个人信息保护包括个性化展示方面的实践做法，以接受公众的监督并与同行交流经验，共同提升我国个人信息保护水平和用户对企业的信任度。

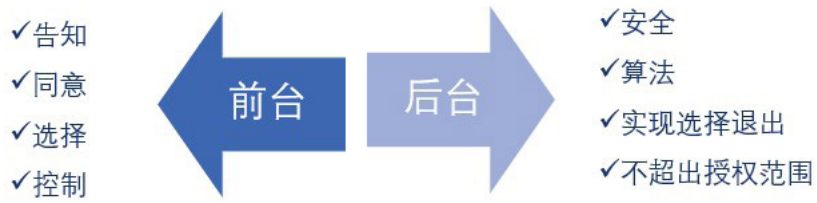
结语

无论从中外立法实践以及相关执法案例，还是从不同业务场景的适用规则，个性化展示的合规与安全治理基本上分为两个层面的保护要求：

其一，确保前台隐私合规。主要包括（1）要对用户进行充分告知，使其拥有其个人信息有可能被用于画像和进而向其进行个性化展示的知情权；（2）让用户自愿表达是否同意其信息被用于画像、被通过画像进行决策（含自动化决策）和针对其个人特征被推送商品、资讯、服务等，需要同时给予拒绝的权利；（3）尊重用户选择的权利，通过透明展示用户的标签，用户可以了解和选择其哪些个人信息被制作画像，可以选择是否被个性化推送，可以选择不想推送基于某些画像标签的商品、资讯、服务，同时还可获得不针对其个人特征选项的商品、资讯、服务；（4）赋予用户选择退出（opt-out）以及选择进入（opt-in）的控制权，包括给予关闭不想收到个性化展示以及不想被形成画像的标签类别。当用户撤回授权时，企业不得代替用户选择在一定时效后自动再打开个性化展示/推送的选项。另外，在用户在关闭标签或者个性化展示功能之后，企业不得再利用用户画像向用户进行推送也不得再将其画像用于其他途径。如有可能，建议企业尽快删除相关标签或者画像，但在删除前可以告知用户一旦选择删除可能产生的相关后果。

其二，确保后台的数据安全。主要包括，企业应当采取与业务发展规模所匹配数据安全保障能力，保障存储与传输中的信息安全。建立有效的防泄露、防篡改机制，做到数据分级分类管理、访问审批权限分明、个人敏感信息加密存储等要求。另外，企业也需要尽合理努力，保证算法的无歧视性，维护消费者公平、合理、公正的权利，不因个性化展示而削弱消费者的基本权利。在前台给予用户选择和控制的同时，后台需要严格配合落实，不得宣称有关闭个性化展示的机制，但实际上在用户关闭后还仍然向其推送或展示基于该用户特征的商品、资讯、服务等，即企业要做到言行一致。最后，对所有后台基于用户个人信息做的行为，包括打标签、推送、与第三方共享数据等，均不应超出企业在隐私政策中声明并且用户授权同意的范围。任何超出授权范围所进行的活动，均应重新告知用户，并获取用户的再次授权同意。

个性化展示的技术越发达，相信人们的生活将越便利。企业应当在发展和鼓励技术革新的同时，严格把好安全与合规的红线，时刻牢记尊重用户的选择，符合用户的隐私期待，争取做越来越好的产品，做负责任的企业。



附录：相关定义列表

个人信息：以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

个人敏感信息：一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

收集：获得对个人信息的控制权的行为，包括由个人信息主体主动提供、通过与个人信息主体交互或记录个人信息主体行为等自动采集，以及通过共享、转让、搜集公开信息间接获取等方式。

用户画像（profiling）：通过收集、汇聚、分析个人信息，对某特定自然人个人特征，如其职业、经济、健康、教育、个人喜好、信用、行为等方面做出分析或预测，形成其个人特征模型的过程。

注：直接使用特定自然人的个人信息，形成该自然人的特征模型，称为直接用户画像。使用来源于特定自然人以外的个人信息，如其所在群体的数据，形成该自然人的特征模型，称为间接用户画像。

自动化决策（automated decision-making）：无任何人工干预的情况下，通过自动化手段做出决策的过程。

个性化展示：基于特定个人信息主体的网络浏览历史、兴趣爱好、消费记录和习惯等个人信息，向该个人信息主体展示信息内容、提供商品或服务的搜索结果等活动。

直接营销（direct marketing）：根据特定用户的特征，通过短信、电话、邮件等方式直接向用户进行营销的行为。

程序化广告或个性化广告：基于特定个人信息主体的网络浏览历史、兴趣爱好、消费记录和习惯等个人信息，以程序化购买广告的方式，通过广告需求方平台、媒介方平台以及广告信息交换平台等所提供的信息整合、数据分析等服务进行有针对性地发布的互联网广告。

北京市环球律师事务所

地　址:北京市朝阳区建国路81号华贸中心1号写字楼15&20层

邮政编码:100025

联系电话:010-65846688

传　真:010-65846666

网　址:www.glo.com.cn

南都个人信息保护研究中心

地　址:曙光西里甲6号院9号时间国际8号楼18层1806室

邮政编码: 100028

联系电话:010-59540274

传　真: 010-59540277

网　址:http://research.nandu.com/piprc/#/

中国信息通信研究院安全研究所

地　址:北京市海淀区花园北路52号

邮政编码:100191

联系电话:010-62305900

传　真:010-62300264

网　址:www.caict.ac.cn